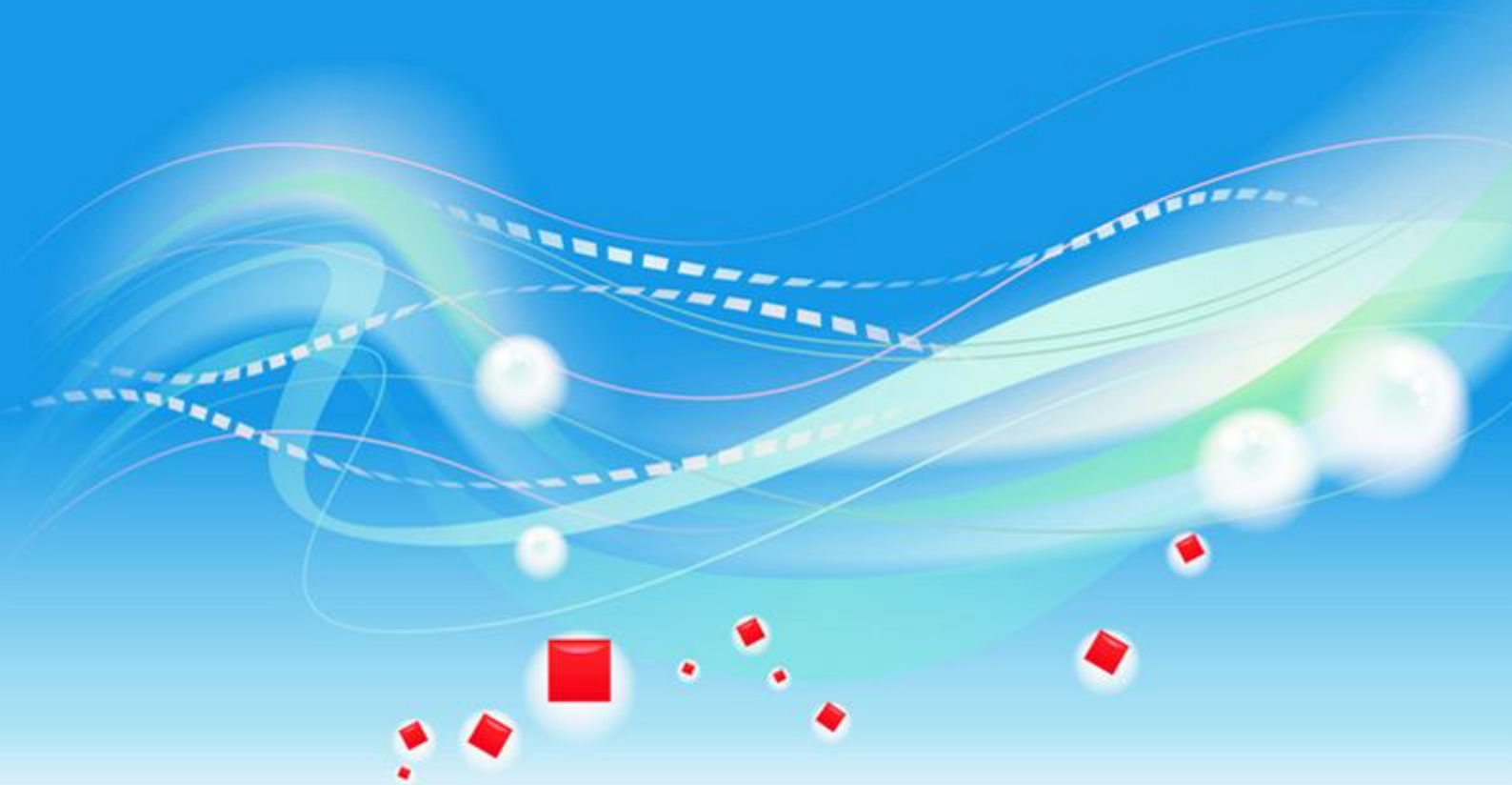

ViPNet CSP 4.0

User's Guide

ViPNet Virtual Private Network

infotecs

© 1991–2013 Infotecs ®. All rights reserved.

Version: 00106-01 34 01 ENU

This document is included in the software distribution kit and is subject to the same terms and conditions as the software itself.

No part of this publication may be reproduced, published, stored in an electronic database, or transmitted, in any form or by any means — electronic, mechanical, recording, or otherwise — for any purpose, without the prior written consent of Infotecs JSC.

ViPNet is a registered trademark of Infotecs JSC, Moscow, Russia.

All brands and product names that are trademarks or registered trademarks are the property of their owners.

Infotecs GmbH

Oberwallstr. 24

10117 Berlin

Deutschland

Tel: +49 (0) 30 206 43 66 0

Fax: +49 (0) 30 206 43 66 66

Email: support@infotecs.biz

Web: http://www.infotecs.biz

Contents

Introduction **8**
About This Document 9
Audience 9
Document Conventions 9
About ViPNet CSP 11
System Requirements 11
Distribution Kit 12
Feedback 13

Chapter 1. Using ViPNet CSP in Data Protection Systems **14**
ViPNet CSP Purpose 15
Encrypting and Signing Documents 16
Key Container 18
Digital Signature 20
Authenticity and Confidentiality of TLS/SSL Connections 21
ViPNet CSP Scope 22

Chapter 2. Quick Start **23**

Chapter 3. Setting Up and Starting ViPNet CSP **25**
ViPNet CSP Setup 26
Running Setup from the Command Line 28
Adding, Uninstalling, and Restoring ViPNet CSP Components 29
Starting ViPNet CSP 31
ViPNet CSP Licensing 33

Chapter 4. Registering ViPNet CSP **34**
Before You Begin 35
Why You Need to Register ViPNet CSP 35
Starting the Registration Process 35
Buying Program (Getting a Serial Number) 37
Requesting a Registration Code 38

Requesting Your Registration Code on the Internet (online) ... 39
Requesting Your Registration Code by Email ... 41
Requesting Your Registration Code by Phone ... 43
Receiving Your Registration Code from the Administrator ... 44
Registering ViPNet CSP ... 47
Saving Registration Data ... 49
If the Configuration of Your Computer Has Been Changed ... 49
System Administrator Actions for Registration Using a File ... 50

Chapter 5. Obtaining a Certificate and Private Key ... 51
Obtaining and Installing a Private Key and a Certificate ... 52
Creating a Certificate Request and Generating a Private Key ... 53
Using Signing Keys of the ViPNet Host's User ... 57

Chapter 6. Installing Containers and Certificates ... 59
Ways to Install a Private Key and a Certificate ... 60
Installing Container from a Folder ... 61
Installing Container from an External Device ... 64
Installing Certificates in a Container ... 66
Installing the User Certificate in the System Store ... 68
Installing a Certificate Which Has Not Been Added to the Container ... 68
Installing a Certificate from Container ... 71
Installing Issuer's Certificates and CRL ... 73

Chapter 7. Working with Containers ... 75
Viewing and Configuring Container Properties ... 76
Changing the Container Password ... 76
Deleting a Previously Saved Password ... 78
Verifying a Key Container ... 78
Deleting a Private Key ... 79
Creating a Backup Copy of a Container ... 81
Deleting a Container ... 82

Chapter 8. Managing External Devices ... 83
Viewing the Connected Devices List ... 84
Configuring the Devices List ... 86
External Device Initialization ... 87

Changing PIN 88
Using a Random Number Generator 89

Chapter 9. Digital Signature in Microsoft Office Documents 91
Digitally Signing a Document 92
Microsoft Office 2003 92
Microsoft Office 2007 93
Microsoft Office 2010 94
Viewing a Digital Signature 96
Microsoft Office 2003 96
Microsoft Office 2007 96
Microsoft Office 2010 97
Removing a Digital Signature 99
Microsoft Office 2003 99
Microsoft Office 2007 99
Microsoft Office 2010 99
Visible Representation of a Signature Line in Word and Excel Documents 101
Adding a Signature Line to a Document 101
Adding a Signature Line to a Document 102

Chapter 10. Digital Signature and Encryption in Microsoft Mail Programs 105
Organizing Encrypted Messages Exchange 106
Exchanging Certificates with the Message Recipient 107
Advanced Configuring of Digital Signature and Encryption 109
Adding a Digital Signature to All Messages 111
Microsoft Outlook 111
Windows Live Mail 113
Adding a Digital Signature to a Message 116
Microsoft Outlook 116
Digitally Sign/Sign Button Isn't Displayed 117
Windows Live Mail 118
Viewing the Message's Digital Signature 119
Microsoft Outlook 119
Windows Live Mail 120
Email Encryption 121
Email Encryption in Outlook 2003 121
Email Encryption in Outlook 2007 122

Email Encryption in Microsoft Outlook 2010 and Microsoft Outlook 2013 123
Email Encryption in the Windows Live Mail Program 125
Viewing the Encrypted Messages 126
Encrypting Documents and Files 127

Chapter 11. Digital Signature in Microsoft Office InfoPath 128
Permission to Sign an InfoPath Form with a Digital Signature 129
Microsoft Office InfoPath 2003 129
Microsoft Office InfoPath 2007 129
Microsoft Office InfoPath 2010 131
Signing an InfoPath Form 133
Microsoft Office InfoPath 2003 133
Microsoft Office InfoPath 2007, 2010, and 2013 134
Viewing an InfoPath Form Signature 136
Unsigning an InfoPath Form 137

Chapter 12. Digital Signature for Macros and Databases 138
Macro Digital Signature 139
Digitally Signing a Macro 139
Verifying a Macro's Digital Signature 140
Unsigning a Macro 141
Signing Microsoft Access 2007 and 2010 Databases 142

Chapter 13. Organizing a Protected Connection via TLS/SSL 144
Checklist: Organizing Access to a Protected Web Server 145
Configuring a Server Host 146
Configuring a Client Host 147
Configuring Internet Explorer for Work over the TLS/SSL Protocol 148
Checking the Web Host's Availability over the Secure HTTPS Protocol 149

Chapter 14. Problems and Troubleshooting 150
Checking the Program Components Integrity 151
The Program Won't Start 152
ViPNet CSP Conflicts with Other Programs 154
Can't Use Accord-TSHM Electronic Lock 156
When You Are Using eToken Aladdin, the System Irresponsive 157
Unable to Check the Certificate 158

Document Can't be Encrypted 159
Email Address of the Certificate Is Not Found on the List of Contact Addresses 159
Invalid Certificate 161
Can't Use the Digital Signature 163
The Corresponding Private Key Is Not Found 163
The Email Message Can't be Signed 163
An Email Message Is Signed with a Certificate That You Have Not Selected for Signing 163
Macros or Microsoft Access 2007 Database Can't be Signed 164
The Signature Line in Microsoft Word 2003 or Excel 2003 Can't be Signed 164
Signed Microsoft Word or Excel Document Can't be Edited 164
No Connection to the Server over HTTPS 165
The IIS Server and the Web Client Have Different ViPNet CSP Versions 165
User's Certificates, the Issuer's Certificate, and CRL Were Installed in the Wrong Store 165
The Browser Is Not Configured to Work over the TLS Protocol 167
The IIS Services Should Be Restarted 168
Password to Server's Certificate Should Be Saved 169
When You Connect to a Server, Security Warning Is Displayed 170
Providing Additional Information About the Problem 171

Appendix A. External Storage Devices 173
Overview 173
Supported External Storage Devices 175

Appendix B. Glossary 177

Appendix C. Index 181

Introduction

About This Document 9

About ViPNet CSP 11

Feedback 13

About This Document

In this document, you can learn about the purpose of the ViPNet CSP program and find how-to topics on its usage. Here you can also get an overview of the ViPNet CSP features, explore the principles of the program operation, and find the description of the graphical user interface.

Audience

This document appeals to those who use certificates in ViPNet CSP for encrypting documents in digital document workflow and Outlook messages, for signing, for digital signatures verification, as well as to system administrators who organize remote access to resources over TLS/SSL protocols.

A ViPNet CSP user does not have to be an information technology professional. However, at least the minimal level of exposure to network technologies, IP protocols, firewalls, and information security is recommended.

Document Conventions

This document concerns the following conventions:

Table 1: Document conventions

Icon	Description
	Warning: Indicates an obligatory action or information which may be critical for continuing user operations.
	Note: Indicates a non-obligatory, but desirable action or information which may be helpful for users.
	Tip: Contains additional information.

Table 2: Conventions for highlighted information

Icon	Description
Name	The name of an interface element. For instance, the name of a window, a box, a button or a key.
Key+Key	Shortcut keys. To use the shortcut keys, press and hold the first key and press other keys.
Menu > Submenu > Command	A hierarchical sequence of elements. For instance, menu items or sections in the navigation pane.
`Code`	A file name, path, text file (code) fragment or a command executed from the command line.

About ViPNet CSP

ViPNet CSP is a cryptographic service provider (see ViPNet CSP Purpose on page 15), which calls cryptographic functions from various Microsoft programs and other programs using the Microsoft CryptoAPI 2.0 interface.

With ViPNet CSP you can:

- Create signature keys (see Digital signature on page 178) in accordance with the GOST R 34.10-2001 and the GOST R 34.10-2012 algorithms.
- Calculate and verify a digital signature in accordance with the GOST R 34.10-2001 and the GOST R 34.10-2012 algorithms.
- Hash data in accordance with the GOST R 34.11-94 and the GOST R 34.10-2012 algorithms.
- Encrypt data and message authentication with modification detection code in accordance with the GOST 28147-89 algorithm.
- Generate random number, pseudo-random numbers, and session encryption keys.
- Authenticate and create the session key when transferring data via SSL/TLS.
- Store public keys certificates directly in the key container.
- Use various tokens and other devices for storing digital keys and certificates securely (eToken and others).

ViPNet CSP is compatible with third-party cryptographic service providers if they comply with RFC 4357 https://tools.ietf.org/html/rfc4357, 4490 https://tools.ietf.org/html/rfc4490, and 4491 https://tools.ietf.org/html/rfc4491.

System Requirements

Note: The compatibility of ViPNet CSP with Windows 7 OS is officially recognized by Microsoft.

The minimum system requirements for your computer to run ViPNet CSP are as follows:

- Processor: Intel Core 2 Duo or any other x86-compatible processor of similar characteristics with two or more cores.
- Minimum RAM: 512 MB.
- Free disk space: 100 MB.
- Operating system: Microsoft Windows XP SP3 (32 bit), Windows Server 2003 (32 bit), Windows Vista (32/64 bit), Windows 7 (32/64 bit), Windows Server 2008 (64 bit), Windows Server 2008 R2 (64 bit), Windows 8 (32/64 bit), Server 2012 (64 bit).

  You must install the latest service pack for your version of Windows.
- Internet Explorer 6.0 or later.
- If Microsoft Office programs are used, the version should be 2003, 2007, 2010, or 2012.

ViPNet CSP is compatible with some external storage devices. For more information about the supported devices, see Supported External Storage Devices (on page 175).

Distribution Kit

The ViPNet CSP distribution kit includes:

- The ViPNet CSP setup file `setup.exe`.
- Document “ViPNet CSP. User's Guide” in PDF format (the current document).
- “ViPNet CSP. Information about Third-Party Software Components.”

Feedback

Finding Additional Information

For more information about Infotecs products and technologies, see the following resources:

- ViPNet documentation web portal http://www.infotecs.biz/doc_vipnet/ENU/index.htm.
- Information about current Infotecs products http://infotecs.biz/products/.
- Information about Infotecs solutions http://infotecs.biz/solutions/.
- Frequently asked questions http://www.infotecs.biz/doc_vipnet/ENU/index.htm#3_17014.htm.

Contacting Infotecs

We value any feedback from you. If you have any questions concerning Infotecs products and solutions, any suggestions, complains or other feedback, feel free to contact us by means of the following:

- Support request form http://infotecs.biz/support/.
- Support email: support@infotecs.biz.
- Telephone: +49 (0) 30 206 43 66 0.
- Fax: +49 (0) 30 206 43 66 66.

Errata

Infotecs makes every effort to ensure that there are no errors or misprints in the text of all documents supplied with ViPNet software. However, no one is perfect, and mistakes do occur. If you find an error in one of our documents, like a spelling mistake or some inaccuracy in describing user scenarios or system features, we would be very grateful for your feedback. By sending in errata you may save other reader hours of frustration, and at the same time you will be helping us provide documentation in even higher quality.

Using ViPNet CSP in Data Protection Systems

ViPNet CSP Purpose	15
Encrypting and Signing Documents	16
Key Container	18
Digital Signature	20
Authenticity and Confidentiality of TLS/SSL Connections	21
ViPNet CSP Scope	22

ViPNet CSP Purpose

The main purpose of the ViPNet CSP cryptoprovider is to enable you to implement cryptographic functions in Windows OS.

Note: Since the cryptographic service provider is an independent software component, you don't need to start any other client ViPNet software for it to work properly.

ViPNet CSP may perform the following tasks:

- Authenticating and ensuring the authenticity of documents in secure document exchange systems. For this purpose, we've implemented the means of digital signatures generation and verification in accordance with GOST R 34.11–94, GOST R 34.11.2012, GOST R 34.10-2001, and GOST R 34.10.2012.
- Ensuring information confidentiality and integrity by encrypting it and using MAC in accordance with GOST 28147–89.
- Ensuring authenticity and confidentiality of TLS/SSL connections.

Encrypting and Signing Documents

To encrypt and verify a digital signature, the ViPNet CSP program employs a public key located in the certificate (see Public key certificate on page 179) of the user the encrypted document is addressed to, or of the user who sent the digitally signed document.

For decrypt or create a digital signature, the cryptographic service provider employs a private key of the user who decrypts or signs the document (the key that is specified by this user).

The scheme below visualizes the process of sending a confidential Outlook message.

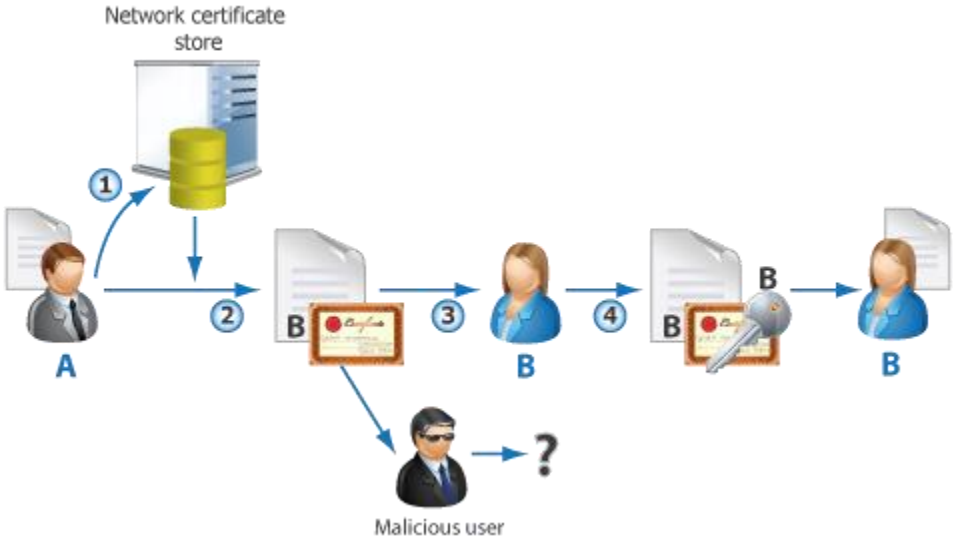

Figure 1: Exchanging protected documents

User **A** needs to send a confidential Outlook message to user **B**.

1. User **A** requests user **B**'s public key certificate from the network certificate store and checks its correspondence with the user **B**'s contact in the Microsoft Outlook program.
2. User **A** encrypts the document using a public key from user **B**'s certificate.
3. User **A** sends the encrypted message to user **B**.
4. User **B** decrypts the document using his or her private key.

   Thus, user **B** receives the confidential message from user **A**.

   If a malicious user intercepts this confidential message, he or she will not be able to read it because he or she does not possess user **B**'s private key.

If user **B** can't decrypt the message received from user **A**, this means that the message has been changed by unauthorized persons or damaged during sending. In this case, user **B** can ask user **A** to resend the message.

The process of digital signature generation and verification is shown below.

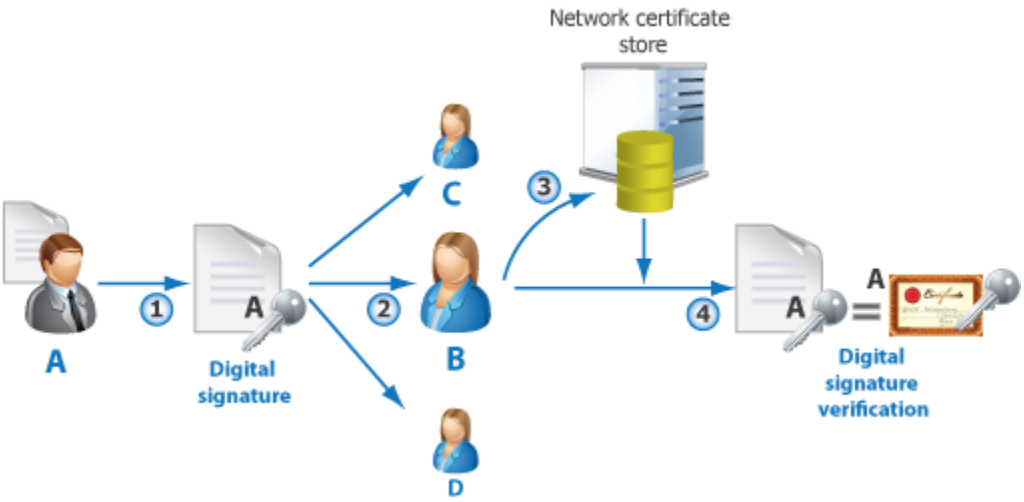

Figure 2: The process of digital signature generation and verification

Suppose that user **A** needs to digitally sign a document (for example, an Outlook message) so that other users can't change it and each user can make sure that the author of the document is user **A**.

1. User **A** signs the document using his or her private key.
2. User **A** sends the document to all persons concerned (to users **B**, **C**, and **D**) or shares the document with them.
3. User **B** requests user **A**'s public key certificate from the certificate store.
4. User **B** verifies the document with user **A**'s public key stored in user **B**'s certificate.

   If verification is successful, the document's author is user **A** and this document has not been changed after signing.

If verification is not successful, the document's author is not user **A** or that the document has been modified by unauthorized persons or damaged during sending. In this case, user **B** can ask user **A** to resend the message.

Key Container

A key pair(a public key and a private key included in a certificate) is used to encrypt and digitally sign documents.

A private key is generated by the administrator in a Certification Authority or by the user. It is stored in a key container on a hard drive or an external device.

A user certificate is created in a Certification Authority on user's request (see Creating a Certificate Request and Generating a Private Key on page 53) or, in some cases, on the Certification Authority administrator's initiative. You can create a certificate request or a renewal request in the client software, such as ViPNet Client, and the Create a certificate request (see Obtaining and Installing a Private Key and a Certificate on page 52) program included in the ViPNet CSP installation package, or a third-party program.

Besides, you need the issuer's certificate (on page 178) chain and CRL (see Certificate revocation list (CRL) on page 177) to validate the user certificate.

To implement a secure electronic document flow system, the program you create electronic documents in (a Microsoft Office program, the Internet Explorer web browser, the IIS) addresses the cryptographic service provider and provides it with the certificates' parameters and location of the private key. For the program to access certificates, you need to install them in the system certificates store:

- You can use the ViPNet CSP program to install the user certificate and the user private key (see Installing Containers and Certificates on page 59).
- You can use standard operating system tools (see Installing Issuer's Certificates and CRL on page 73) to install the issuer's certificate and CRL.

ViPNet CSP allows you to install private keys and public key certificates in the following ways:

- Adding a container with a private key and a certificate. The container may be located in a folder on a disk (see Installing Container from a Folder on page 61) or on an external device (see Installing Container from an External Device on page 64).
- Installing the certificate and choosing the corresponding private key from the container in a folder on a disk or on an external device (see Installing the User Certificate in the System Store on page 68).

A certificate can be stored separately from a private key in cases when the certificate is created on a user's request. A certificate and a private key are stored in the same container when the certificate request is initiated by the Certification Authority administrator.

A container format depends on the particular cryptographic service provider's vendor. Certificate files are always created only in the following standard formats:

- X.509 format, containing only a certificate (files with extensions `.crt` or `.cer`).
- PKCS#7 or PKCS#12 formats. These formats are intended for storing encrypted and signed messages together with the necessary certificates. One of these file formats can also be used for transferring certificates and certificate revocation lists (files with extensions `.p7r`, `.p7b`, `.pfx`, and `.p12`).

Note: You can use any number of certificates and key containers in ViPNet CSP. In this case, to digitally sign a document, you need to choose the key, which you will use.

Digital Signature

The digital signature is an attribute of an electronic document that is a result of cryptographic data processing with the use of a private key.

A digital signature can confirm:

- Authenticity. A digital signature unambiguously identifies the person who has signed the document.
- Integrity. A digital signature confirms that the document has not been changed after the signing.
- Non-repudiation. The author can't deny the fact that he or she has signed the document.

Thus, individuals and legal entities may use a digital signature as an equivalent to a handwritten signature to ensure the legal validity of an electronic document equal to the legal validity of a printed or handwritten document signed manually by the eligible person and officially sealed.

To use a digital signature, you need to get a public key certificate (see Key Container on page 18) in a competent Certification Authority.

If certificate validation with the use of the Certification Authority's database confirms that a certificate is legal, functional, has not expired, and has not been revoked, this certificate is considered valid. The documents that are signed using a valid certificate and have not been changed since the moment of signing are considered valid as well.

Authenticity and Confidentiality of TLS/SSL Connections

The TLS/SSL protocol is used to organize remote protected connections, for example, to get access to remote server's resources. The TLS/SSL protocol ensures performing of one-way authentication or mutual authentication for interacting parties, as well as confidential data transfer. You may need secure access when you share databases or repositories, or create electronic payment systems, and for some other functionality.

The interaction between two hosts in a protected connection is displayed in the scheme below.

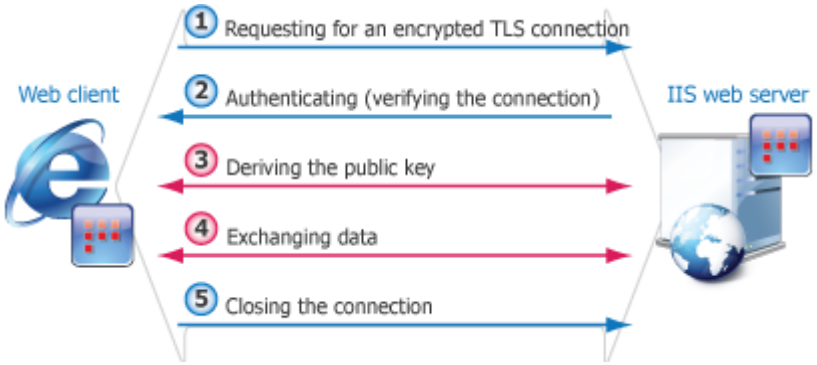
1 Requesting for an encrypted TLS connection
Web client
2 Authenticating (verifying the connection)
IIS web server
3 Deriving the public key
4 Exchanging data
5 Closing the connection

Figure 3: Hosts communicate over TLS

Note: Beside Microsoft Internet Explorer, you may use Google Chrome or Yandex.Browser as a web client. Therefor, in the browser's shortcut properties, in the **Object** box, at the end of the path to the program folder add the command `--use-system-ssl`.

Thus, the usage of the TLS/SSL protocol implemented by means of ViPNet CSP provides a reliable and authorized connection to remote servers and strictly controlled access to the protected data.

ViPNet CSP Scope

With ViPNet CSP you can perform the following operations:

- encrypt Microsoft Outlook, Microsoft Outlook Express, Microsoft Windows Mail, and Microsoft Windows Live Mail messages and their attachments (see Email Encryption on page 121);
- generate and verify a digital signature in Microsoft Office programs (see Digital Signature in Microsoft Office Documents on page 91);
- sign Microsoft Outlook, Microsoft Outlook Express, Microsoft Windows Mail, and Microsoft Windows Live Mail messages (see Digital Signature and Encryption in Microsoft Mail Programs on page 105);
- sign Microsoft Office InfoPath forms (see Digital Signature in Microsoft Office InfoPath on page 128);
- sign macros in Microsoft Word, Excel, Outlook, PowerPoint, Access, Publisher, and Visio programs (see Macro Digital Signature on page 139);
- establish protected TLS/SSL web connections by using an IIS server and the Microsoft Internet Explorer browser (see Organizing a Protected Connection via TLS/SSL on page 144);
- perform cryptographic functions in the DocVision electronic document workflow;
- authenticate in Windows with the Kerberos protocol;
- perform cryptographic operations required for Active Directory Certificate Services.

Quick Start

If you need to secure electronic documents by means of cryptography and to digitally sign documents, ensuring their authenticity and integrity, you should install a special module called a cryptographic service provider (see ViPNet CSP Purpose on page 15).

To start using the cryptographic service provider ViPNet CSP:

1. Install ViPNet CSP (see ViPNet CSP Setup on page 26).
2. Get a public key certificate and a container with a private key:
   - Your Certification authority administrator may have given you a certificate file and a container file with a private key (or a container file containing both a private key and a certificate) earlier. Make sure that you already have these files.
   - If you don't have a container or a certificate, create a certificate request (see Obtaining and Installing a Private Key and a Certificate on page 52).

   Together with the certificate and the key container, you receive the issuer's certificate (on page 178) and the certificate revocation list (CRL) (on page 177).

Note: A certificate contains a public key corresponding to only one private key. The private key is stored on a user's computer and is used to generate a digital signature and to decrypt encrypted messages. A public key is used to verify a digital signature and to encrypt messages, and it is distributed in a certificate.

The issuer's certificate and CRL are used to verify the authenticity of your certificate.

3 Install a public key certificate and the corresponding private key (or several certificates and keys) (see Ways to Install a Private Key and a Certificate on page 60).

Note: When you add a container, you will be prompted to install the certificate into the system store. If the certificate has not been installed, you should do it manually (see Installing a Certificate from Container on page 71).

4 Install the issuer's certificate and a certificate revocation list (see Installing Issuer's Certificates and CRL on page 73) in the system store.

Note: If you are a web server administrator and you want to organize a secure connection to your server over TLS/SSL, configure the server and web clients for work over the TLS/SSL protocol (see Organizing a Protected Connection via TLS/SSL on page 144) .

5 Upon completing the above-mentioned steps, you may use any programs that use a cryptographic service provider in their work (see ViPNet CSP Scope on page 22). These can be programs for working with a digital signature, encryption, secure communication, and others.

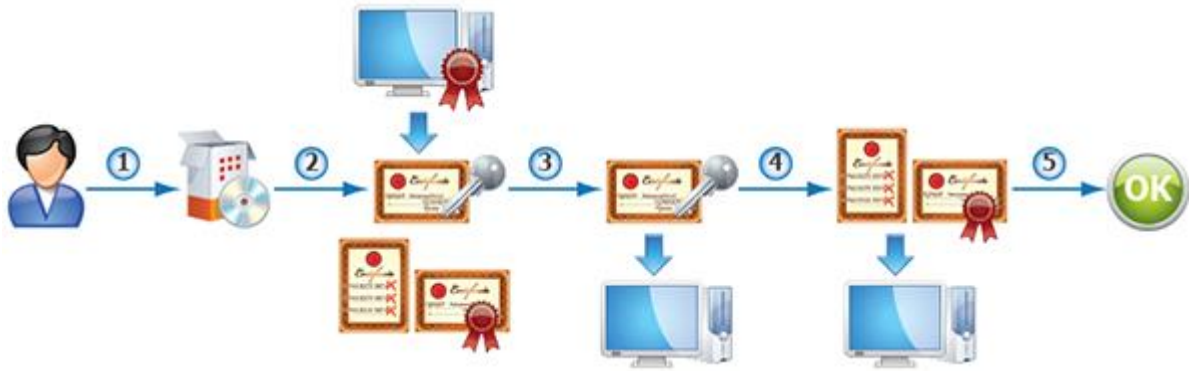

Figure 4: Start using ViPNet CSP

3

Setting Up and Starting ViPNet CSP

ViPNet CSP Setup	26
Running Setup from the Command Line	28
Adding, Uninstalling, and Restoring ViPNet CSP Components	29
Starting ViPNet CSP	31
ViPNet CSP Licensing	33

ViPNet CSP Setup

If the ViPNet CSP program is part of ViPNet software, it is installed together with this software.

If you need to install program separately, follow the instructions in this section. To install ViPNet CSP, you should have OS administrator rights on your computer.

To install ViPNet CSP:

1. Double-click the setup file .
2. On the **License** page of the setup program, read the terms and conditions of the license agreement. If you agree, select the corresponding check box. Then click **Continue**.
3. To configure the setup parameters, on the **Setup type** page, click **Customize** and specify:
   - the software components you want to install;
   - the path to the program folder on your computer;
   - the user name and the company name;
   - the name of the program folder on the **Start** menu.

   You can enable or disable the following software components:
   - **ViPNet CSP support via MS Cypto API** adds the functionality that allows you to integrate ViPNet CSP in third-party programs. This component is enabled by default when you install ViPNet CSP as a separate program and disabled when you install it as a part of some other ViPNet software.
   - **KC3 integrity check** adds the functionality that ensures file integrity check. This is required so that ViPNet CSP conforms with the KC3 Russian standard for cryptographical protection.
4. To start the setup, click **Install now**.
5. You will be prompted to restart your computer. To restart the computer immediately, click **Yes**.

To register ViPNet CSP during installation without displaying the user interface ("Silent mode"), you need to prepare the registration file `cspreg.txt` and put it to the same folder as the `setup.exe` file. The `cspreg.txt` file must be as follows:

```
Serial Number: XXXX-XXXX-XXXX-XXXX
```

```
E-mail: email@infotecs.ru
User name: <User first, second, and last name>
Company: <Company name>
```

Note: The `User name` and `Company` fields are optional.

Running Setup from the Command Line

You may run ViPNet CSP setup program from the Windows command line specifying a number of standard Windows Installer arguments.

Table 3: Setup mode arguments

Argument	Description
`/qn`	Installation without displaying user interface (“Silent mode”).
`/qb`	Installation with basic user interface (only a standard indicator of progress and informational messages are displayed).
`/qf`	Installing with full user interface (default).

Table 4: Restart mode arguments

Argument	Description
`/norestart`	Disable restart after installation.
`/promptrestart`	Display a dialog box prompting you to restart.
`/forcerestart`	Restart the computer after installation and force other applications to close without saving opened files. This parameter is valid only in conjunction with the `/qn` argument.

Here is an example of the setup command:

```
setup.exe /qn /norestart
```

Adding, Uninstalling, and Restoring ViPNet CSP Components

If necessary, you can install or uninstall ViPNet CSP components and restore the software in case of a failure. To add or remove a component or to restore ViPNet CSP:

1. Run the setup file . Wait until the preparation for the components' installation is completed.
2. In the **Changing installed software components** window, click the required option:
   - to add or remove a component, click **Add or remove components**;
   - to restore the program, click **Restore**;
   - to remove all components of the program, click **Remove All Components**.

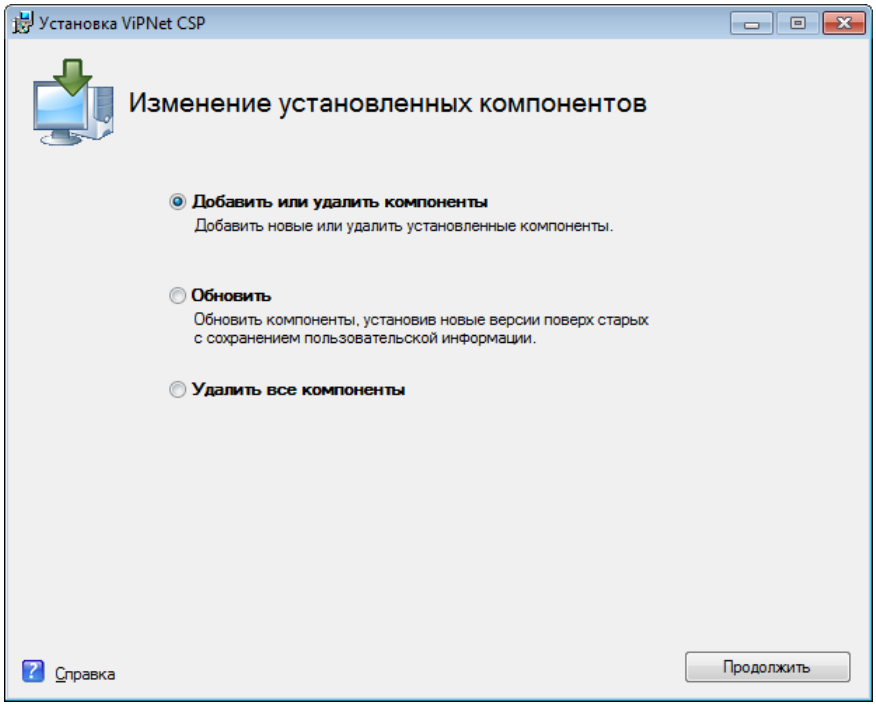

Figure 5: Changing installed software components

Then, click **Continue**.

3 If you add or remove any ViPNet software components, make the necessary changes in the **Choose components** window. Then, click **Continue**.

4 Wait for the operation to be completed. Then, click **Close**.

Starting ViPNet CSP

To configure the ViPNet CSP program, do one of the following:

- Click the **Start** button, choose **All Programs** > **ViPNet** > **ViPNet CSP** > **ViPNet CSP Settings** (the program location on the **Start** menu might have been changed at installation).
- On the desktop, double-click the shortcut (this shortcut is displayed only if the corresponding option has been selected during the installation).

When you start **ViPNet CSP** demo version, you will be offered to register the program. You may register the program or run a demo version (see ViPNet CSP Licensing on page 33).

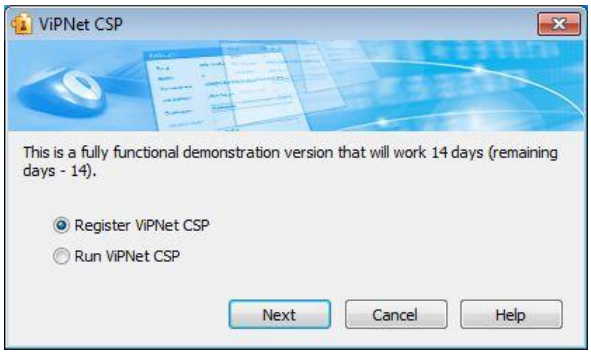

Figure 6: Starting a demo version

After the ViPNet CSP startup, the **General** section of the main window will be displayed. This section contains information about the program version, license owner, and ViPNet CSP operation mode.

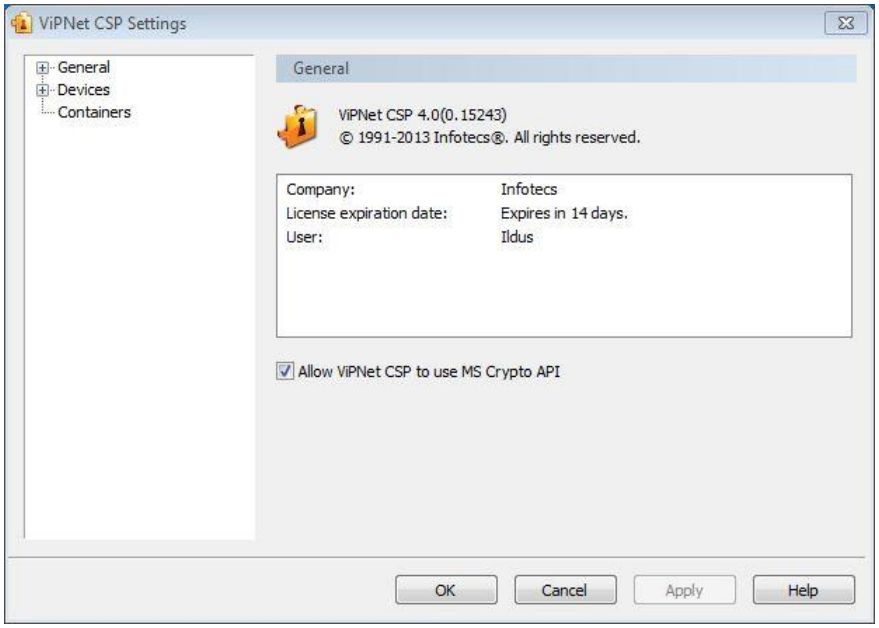

Figure 7: Displaying information about ViPNet CSP

Started using ViPNet CSP. First, we recommend you to install a key container and a certificate. (see Installing Containers and Certificates on page 59)

ViPNet CSP Licensing

If you install the ViPNet CSP program as part of another ViPNet software, registration is not required. If you install the ViPNet CSP separate, you need to register it.

Using a demo license, you can work with ViPNet CSP only for 14 days. After that the program will stop functioning and you will need to register it. However, there are no limitations in the demo version, and all features are available.

You can register ViPNet CSP for free so we strongly recommend you to do it as soon as possible to avoid any inconvenience when demo period expires.

When the demo period expires, you can't work with unregistered ViPNet CSP program. To continue the work, you need to register the program (see Registering ViPNet CSP on page 34). The registration is free.

Registering ViPNet CSP

Before You Begin	35
Buying Program (Getting a Serial Number)	37
Requesting a Registration Code	38
Registering ViPNet CSP	47
System Administrator Actions for Registration Using a File	50

Before You Begin

Why You Need to Register ViPNet CSP 35

Starting the Registration Process 35

Why You Need to Register ViPNet CSP

After you install ViPNet CSP, it starts in the demo mode and you can use it only for a limited period of time (see ViPNet CSP Licensing on page 33). If you find that ViPNet CSP meets your requirements, you should register it to enjoy a full-featured version.

That is why we recommend you the following workflow:

- install ViPNet CSP and feel free to use the demo version to find out all its features and advantages;
- When the validity period of your demo license expires, you need to register your ViPNet CSP copy.

Starting the Registration Process

ViPNet CSP can be registered in two ways: by yourself (common registration) and by the system administrator. To register by yourself, follow the scenario below.

If you are a system administrator and you need to register several copies at once, you can use the group registration feature allowing you to collect several users' registration requests in one e-mail and receive all required registration codes at once. For more information, see System Administrator Actions for Registration Using a File (on page 50).

Note: If ViPNet CSP has been reinstalled and registered on your computer, you can restore the previously saved registration data using the `*.brg` file (see Saving Registration Data on page 49).

If you are planning to perform minor upgrades to the computer, where you are going to use ViPNet CSP, consider the topic If the Configuration of Your Computer Has Been Changed (on page 49).

To register ViPNet CSP:

1 In the ViPNet CSP main window, on the **Help** menu, click **Registration**. **The Registration of ViPNet CSP Wizard** will be launched.

ViPNet CSP Registration Wizard
ViPNet CSP Registration Wizard
Welcome to the wizard that will help you to register ViPNet CSP.
To register the program, you should get a serial number. If you already have a serial number, you should request a registration code from Infotecs. After that you can register the program. Select an appropriate option and click Next.
Get the serial number (free of charge)
Request registration code
Register program
< Back
Next >
Cancel
Help

Figure 8: First registration page

2 Your next step depends on whether you have got the ViPNet CSP serial number beforehand:

- If you have not got the serial number, click **Get the serial number (free of charge)** (see Buying Program (Getting a Serial Number) on page 37).
- If you have got the serial number, click **Request registration code** (see Requesting a Registration Code on page 38).

Note: If you request your registration code online, your ViPNet CSP registration will be done automatically (no user action is required).

- If you have already got both the serial number and the registration code, click **Register** (see Registering ViPNet CSP on page 47).

Buying Program (Getting a Serial Number)

To buy a serial number:

1. In the**The Registration of ViPNet CSP** wizard, select **Get the serial number (free of charge)**, and click **Next**.

   The ViPNet products order page on the Infotecs website will be displayed in your default Internet browser.

2. Choose the product version, fill in the request form an send it. The link to download the product and the serial number will be sent to your email.

3. Upon receiving a serial number, return to the **Registration of ViPNet CSP** (see Starting the Registration Process on page 35) wizard and request a registration code (see Requesting a Registration Code on page 38).

Requesting a Registration Code

To request a registration code for ViPNet CSP:

1. On the **Registration of ViPNet CSP** page, choose **Request registration code** and click **Next**.
2. On the **Registration request options** page, choose the means of requesting your registration code. To do this, choose one of the following options:
   - **On the Internet (online)** (see Requesting Your Registration Code on the Internet (online) on page 38).
   - **By email** (see Requesting Your Registration Code by Email on page 41).
   - **By phone** (see Requesting Your Registration Code by Phone on page 43).
   - **Using file** (see Receiving Your Registration Code from the Administrator on page 44).

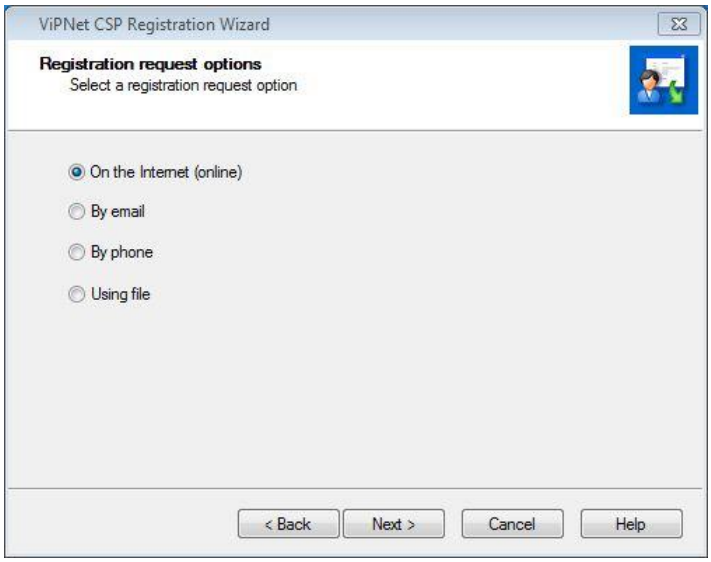

Figure 9: Selecting a registration request option

3. Click **Next**.

Requesting Your Registration Code on the Internet (online)

Warning: For requesting a registration code on the Internet you need an Internet connection.

If you select **On the Internet (online)**, the **Registration data** page will be displayed.

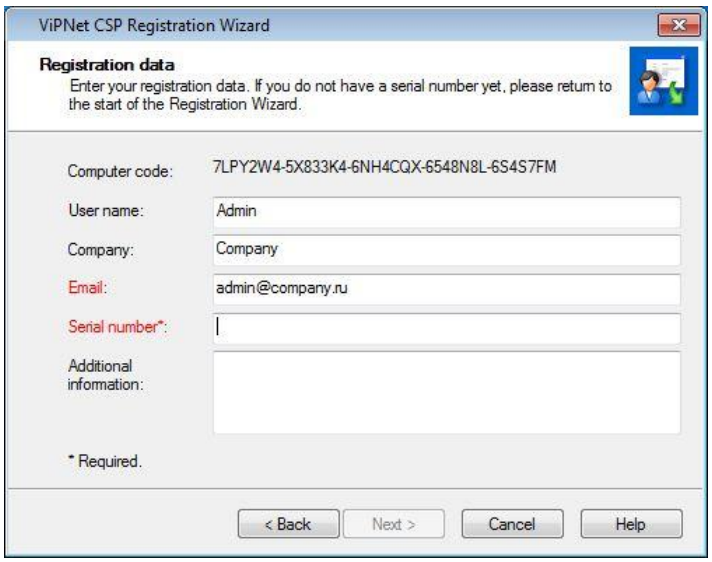

Figure 10: Entering registration data

On the **Registration data** page:

1 In the **Serial number** box, type your serial number.

Note: If you do not have a serial number, make request to purchase it (see Buying Program (Getting a Serial Number) on page 37).

If you have ever previously typed your serial number in this box, your serial number will be entered automatically.

2 In the **User name** box, type your name to be used when issuing your license and contacting you. This box is optional. By default, the user name you have typed at the ViPNet CSP installation will be displayed.

3 In the **Company** box, type your company name. This box is optional. By default, the company name you have typed at the ViPNet CSP installation will be displayed.

4 In the **Email** box, type your e-mail address which will be used to contact you in case of need.

Warning: We will not sell, distribute or lease your e-mail addresses. We are committed to ensuring that your information is secure. In order to prevent unauthorized access or disclosure we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect from you.

5 In the **Additional information** box, feel free to type any additional information. For example, you can type here how to contact you or post some problems or suggestions on ViPNet registration utility or ViPNet software in the whole.

In the **Computer code** box, a code that uniquely identifies your computer is displayed. You can't change this value.

6 Click **Next**. The page, showing your registration request status, will be displayed. On this page you will also see how much time elapsed since you had begun your registration request. Please note, that you have no more than three minutes to complete your online registration request.

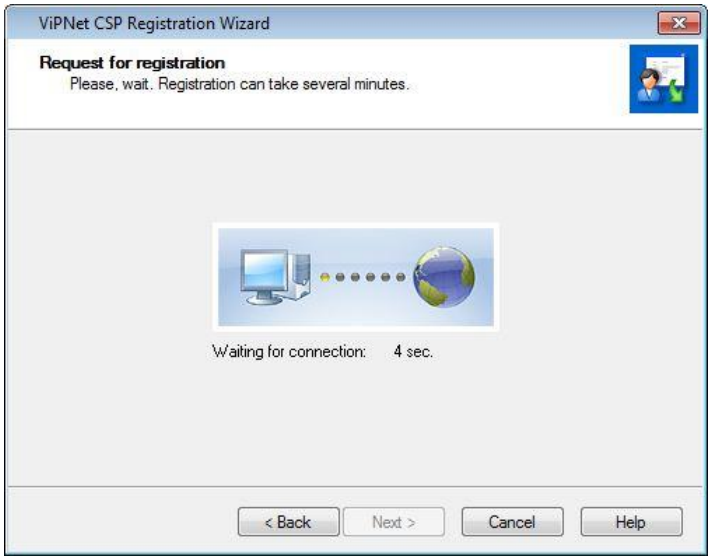

Figure 11: Requesting for registration

If within the three minutes a connection to the Infotecs registration server is not established, the corresponding message will be displayed.

If a connection to the Infotecs registration server is established, the registration may failed by the following reasons:

- You have supplied incorrect data. In this case, you will be prompted to check the correctness of supplied data.

  In the message window, click **OK** to return to the **Registration data** page.

- The entered serial number has been already registered for another computer. In this case, you will be prompted to to get another serial number free of charge.

  Click the link in the message and request a new serial number (see Buying Program (Getting a Serial Number) on page 37).

If online registration was successful, the **Registration of ViPNet CSP was successful** page will be displayed. This page will also display some suggestions on how to securely backup your registration data (see Saving Registration Data on page 49).

7 Click **Finish**.

Requesting Your Registration Code by Email

Warning: For requesting a registration code on the Internet you need an Internet connection.

If you select **By email**, the **Registration data** page will be displayed. On the **Registration data** page:

1 Provide all your data as described in Requesting Your Registration Code On the Internet (Online) (on page 38).

2 Click **Next**. An email summarizing your registration data will be automatically opened in your default email application. It will be addressed to reg@infotecs.biz.

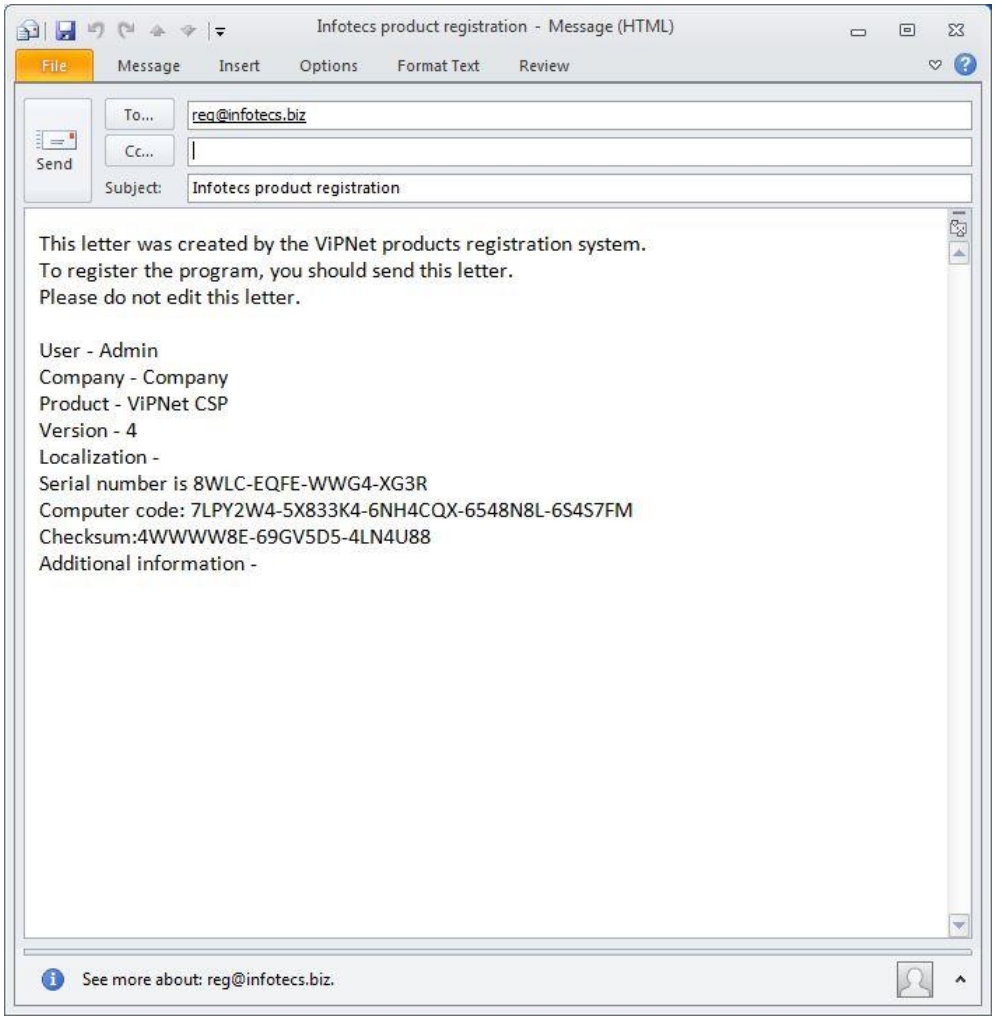

Figure 12: Requesting registration code by email

Warning: We don't recommend you to modify anything in this auto-generated email.

3 To complete the procedure, send this email. When Infotecs has checked your registration data, you will receive your registration code in response.

Warning: If you don't receive a response e-mail from Infotecs for a long period of time, you may try to resend your email. To do this, repeat all steps described in this topic. If you still can't register your ViPNet CSP, contact Infotecs Support Team.

4 Upon receiving a response email with registration code, register your ViPNet CSP (see Registering ViPNet CSP on page 47).

Requesting Your Registration Code by Phone

If you select **By phone**, the **Registration request by phone** page will be displayed.

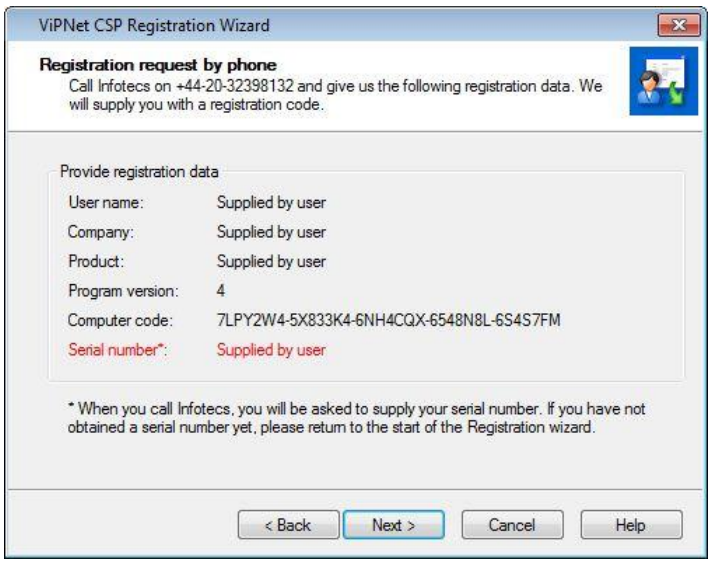
ViPNet CSP Registration Wizard
Registration request by phone
Call Infotecs on +44-20-32398132 and give us the following registration data. We will supply you with a registration code.
Provide registration data
User name: Supplied by user
Company: Supplied by user
Product: Supplied by user
Program version: 4
Computer code: 7LPY2W4-5X833K4-6NH4CQX-6548N8L-6S4S7FM
Serial number*: Supplied by user
* When you call Infotecs, you will be asked to supply your serial number. If you have not obtained a serial number yet, please return to the start of the Registration wizard.
< Back
Next >
Cancel
Help

Figure 13: Registration request by phone

This page displays all the data you need to tell Infotecs.

1 Call Infotecs on the phone number specified at the top of the window and request a registration code.

2 When you receive the registration code, click **Next**. The **Register** page will be displayed.

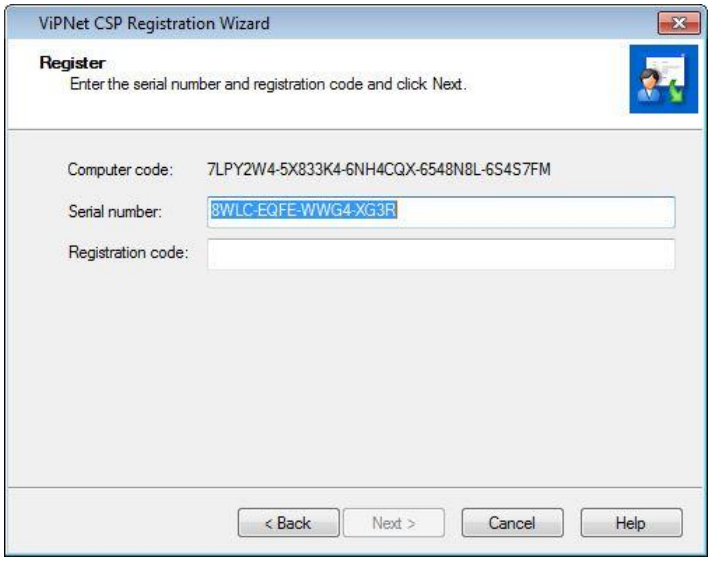

Figure 14: Entering the serial number and registration code

3 On the **Register** page type your serial number and registration code, then click **Next**.

Note: If you have ever previously typed your serial number in this box, your serial number will be entered automatically.

If you provided correct data, the **Registration of ViPNet CSP was successful** page will be displayed. This page will also display some suggestions on how to securely backup your registration data (see Saving Registration Data on page 49).

4 Click **Finish**.

Receiving Your Registration Code from the Administrator

The idea behind registering using a file is to delegate the registration code receiving process to your ViPNet network administrator. This means that you personally don't request your registration code from Infotecs. Instead you use the **Registration of ViPNet CSP Wizard** to collect your registration data and then pass it to your ViPNet network administrator.

Note: If you would like to register only one copy of ViPNet CSP using a file, first complete actions 1–6 described in this chapter and then follow the instructions given in the chapter System Administrator Actions for Registration Using a File (on page 50). Then, complete the step 7 to register your copy of ViPNet CSP (see Registering ViPNet CSP on page 47).

It is your ViPNet network administrator, who collects your and other ViPNet users' registration data and sends it to Infotecs. It is your ViPNet network administrator, who obtains your and other ViPNet users' registration codes and then passes them to you and your fellow ViPNet users. Upon receiving your registration code from your ViPNet network administrator you can register your ViPNet CSP.

To register your ViPNet CSP using a file:

1. On the **Registration request options** page, choose **Using file**. The **Registration data** page will be displayed.
2. Provide all your data as described in Requesting Your Registration Code on the Internet (online) (on page 38). Click **Next**.
3. On the **Saving registration data** page, click **Browse** and select the folder that will store the file containing your registration data.

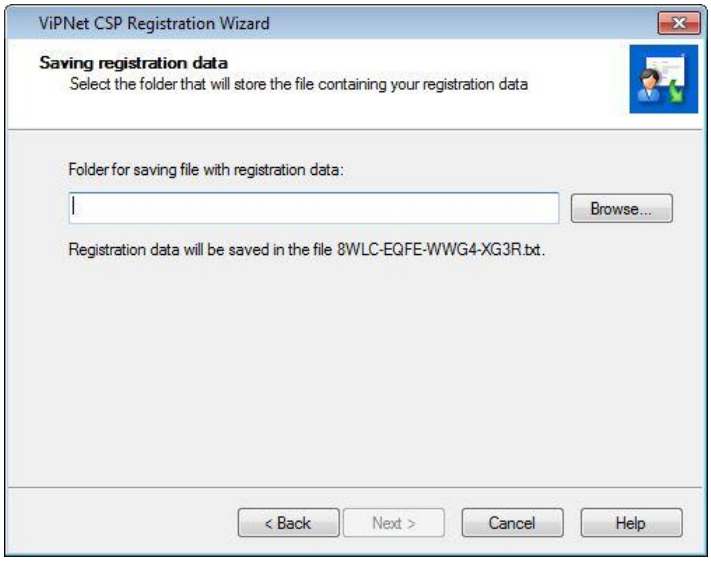
ViPNet CSP Registration Wizard
Saving registration data
Select the folder that will store the file containing your registration data
Folder for saving file with registration data:
Browse...
Registration data will be saved in the file 8WLC-EQFE-WWG4-XG3R.txt.
< Back
Next >
Cancel
Help

Figure 15: Saving registration data

4. Click **Next**. The registration data is saved in a text file named after the serial number of the program: `<serial number>.txt`.

ViPNet CSP Registration Wizard
Inform your system administrator that you have created a file containing registration data. Once you receive a registration code from your system administrator, you can register ViPNet CSP. If you have any questions about registration using a file, please contact your system administrator.
If you have other questions don't hesitate to contact Infotecs:
Web: http://www.infotecs.biz
E-mail: support@infotecs.biz
< Back
Next >
Finish

Figure 16: Registration data have been saved

5 Click **Finish**.

6 Send the file containing your registration data to your system administrator.

7 When you receive your registration code from your system administrator, register your ViPNet CSP (see Registering ViPNet CSP on page 47).

Registering ViPNet CSP

Upon receiving registration code from Infotecs, you can register your ViPNet CSP. To do this:

1 Launch the **Registration of ViPNet CSP** (see Starting the Registration Process on page 35).

2 On the first wizard page, choose **Register program** and click **Next**.

3 On the **Serial number** page, type your serial number.

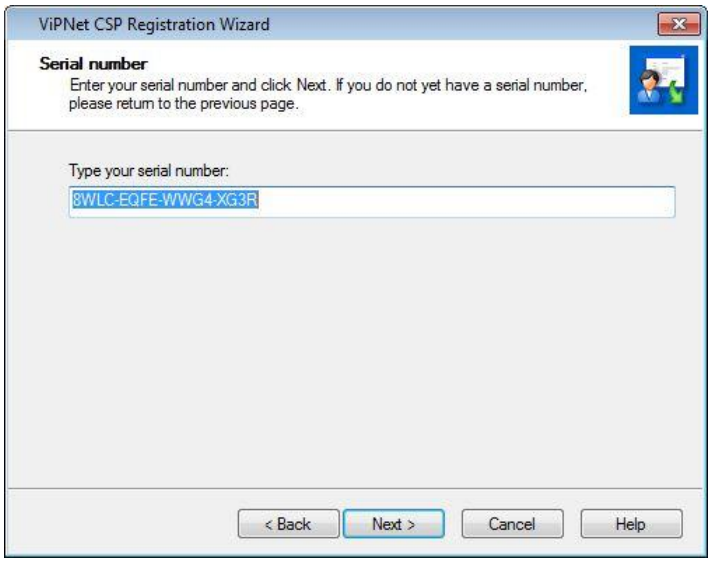
ViPNet CSP Registration Wizard
Serial number
Enter your serial number and click Next. If you do not yet have a serial number, please return to the previous page.
Type your serial number:
8WLC-EQFE-WWG4-XG3R
< Back
Next >
Cancel
Help

Figure 17: Entering a serial number

Note: If you have ever previously typed your serial number in this box, your serial number will be entered automatically.

4 On the **Registration Code** page:

- you personally sent a request for a registration code, select **Single registration** and type the registration code.
- your system administrator sent a request for a registration code, select **Using file**, click **Browse** and locate the file on your network that contains the registration code.

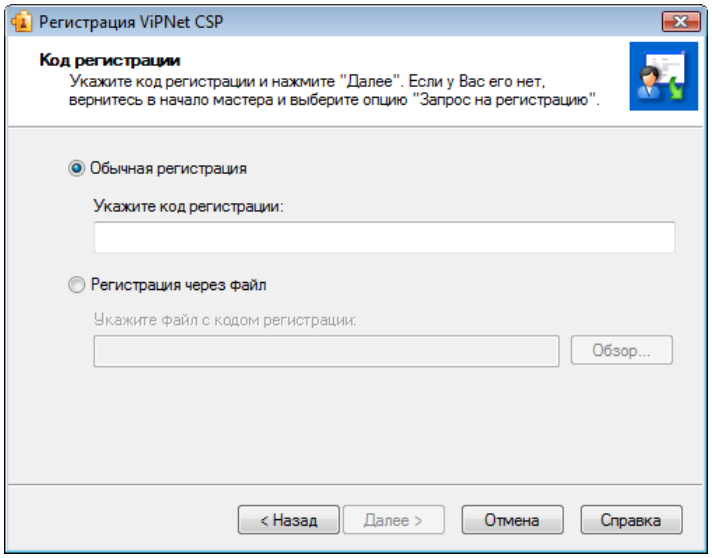

Figure 18: Ввод кода регистрации

5 Click **Next**. If you provided correct data, the **Registration of ViPNet CSP was successful** page will be displayed:

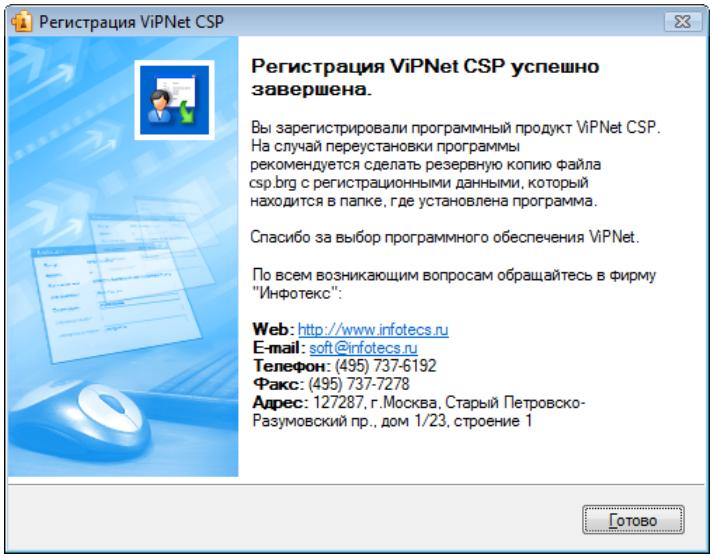

Figure 19: Завершение регистрации

6 Click **Finish**.

7 Back up your registration data (see Saving Registration Data on page 49) by copying your registration file to a secure location. The file `offmanager.brg` is located in the same folder as the ViPNet CSP application.

Saving Registration Data

The registration process saves registration data to the `*.brg` file, which is created in one of the following folders:

- `C:\ProgramData\infotecs\ViPNet CSP\` for the operating systems Windows Vista, Windows 7 and Windows Server 2008;
- `C:\Documents and Settings\All Users\Application Data\infotecs\ViPNet CSP\` for the operating systems Windows XP and Windows Server 2003.

Note: The name of the `*.brg` file depends on the ViPNet program version.

We recommend you to save this file in a secure place because it will be useful in some cases of re-installation (for example, if you need to install the program into another folder on your computer, or you need to re-install the program after formatting your hard drive). In such cases, you should unload the program, move the saved `*.brg` file back into the folders mentioned above, and then start the program anew. Upon start, ViPNet CSP will be registered automatically (as long as the registration data are valid and the configuration of your computer has not changed).

Registration data (serial number, computer code, registration code, and more) is also stored in a registration log file named `reginfo.txt`, located in the ViPNet CSP installation folder. You can use information from this file for manual registration of the program after re-installation (for example, if the `*.brg` file has been lost).

If the Configuration of Your Computer Has Been Changed

Changes in computer configuration may influence the work of ViPNet Network Manager installed on this computer. If your upgrade was substantial (you replaced almost all hardware in your PC) you will need to register your ViPNet Network Manager once again (see Requesting a Registration Code on page 38). If you made only minor changes to your computer's configuration, you will not have to register your ViPNet Network Manager again.

At the first ViPNet Network Manager startup after minor upgrade the message will be displayed informing you that your computer's configuration has been changed and a new `*.brg` file has been created. This means that your previous registration data became obsolete. You will not be able to register your ViPNet Network Manager using those data after its reinstallation.

That is why you should copy this updated `*.brg` file into the secure location. If you reinstall ViPNet CSP on this computer, you should copy this very file to the ViPNet CSP installation folder. Only after that the application will consider itself registered.

System Administrator Actions for Registration Using a File

Registration using file allows a company to request and receive registration codes for several users via a single person. This person is normally the organization's system administrator.

To register using file, all ViPNet users must have their product's serial number. If not, they need to buy it via the **Registration of ViPNet CSP** (see Buying Program (Getting a Serial Number) on page 37).

Each user, from their computer, should have created a using file registration request (see Receiving Your Registration Code from the Administrator on page 44). This creates a `*.txt` file containing registration data, which they will send to their system administrator.

If you are a system administrator:

1. Save the files obtained from ViPNet users and containing their registration data to the same folder.
2. When you have them all, combine them using the copy command: `copy *.txt registration.all`. You can use another file name instead of `registration.all`.
3. Email the file to Infotecs at reg@infotecs.biz. Name the email “ViPNet Registration Using File”.
4. After Infotecs company has processed the request, you will receive an email with an attached `*.txt` file. This file will contain registration codes for all users taking part in the group registration. Deliver this file to users (for example via network disk) who can then register their installed ViPNet program.

5

Obtaining a Certificate and Private Key

Obtaining and Installing a Private Key and a Certificate 52

Creating a Certificate Request and Generating a Private Key 53

Using Signing Keys of the ViPNet Host's User 57

Obtaining and Installing a Private Key and a Certificate

To have an opportunity to sign electronic documents, you need to get a user private key, and to verify a digital signature, you need to get a public key certificate.

Note: The order of obtaining and commissioning a certificate and private key is determined by the rules of your Certification Authority. To generate a certificate request, ask your Certification Authority's administrator whether requests, generated in the Create a certificate request program, will be accepted.

To obtain and to commission a new certificate or to renew already existing certificate, you need to:

1. Create a certificate request in the Create a certificate request program (see Creating a Certificate Request and Generating a Private Key on page 53).
2. Create a private key or save a container with the private key on the disk or an external device.
3. Send the certificate request file to your Certification Authority's administrator (by e-mail or other means used in your company) and wait until you receive the certificate.
4. Install the received certificate in a container (see Installing Certificates in a Container on page 66).
5. Install the received certificate (see Installing the User Certificate in the System Store on page 68), the issuer's certificate and CRL (see Installing Issuer's Certificates and CRL on page 73) in the system store.

Creating a Certificate Request and Generating a Private Key

To create a request for a new certificate or to renew an existing certificate:

1. On the **Start** menu, click **All programs** > **ViPNet** > **ViPNet CSP** > **Create a certificate request**.
2. In the **Certification Authority** window, choose one of the following:
   - **Request new certificate** to create a new certificate request.
   - **Request a renewal of the existing certificate** to renew an existing certificate. When you are creating a certificate renewal request:
     - In the **Renew Certificate** window, select the certificate to be renewed and click **OK**.
     - If you need to select another certificate or view the selected certificate, use the **Select certificate** and **Selected certificate** buttons.
     - If necessary, specify new certificate parameters and details about the owner of the certificate or use the details of the previous certificate.

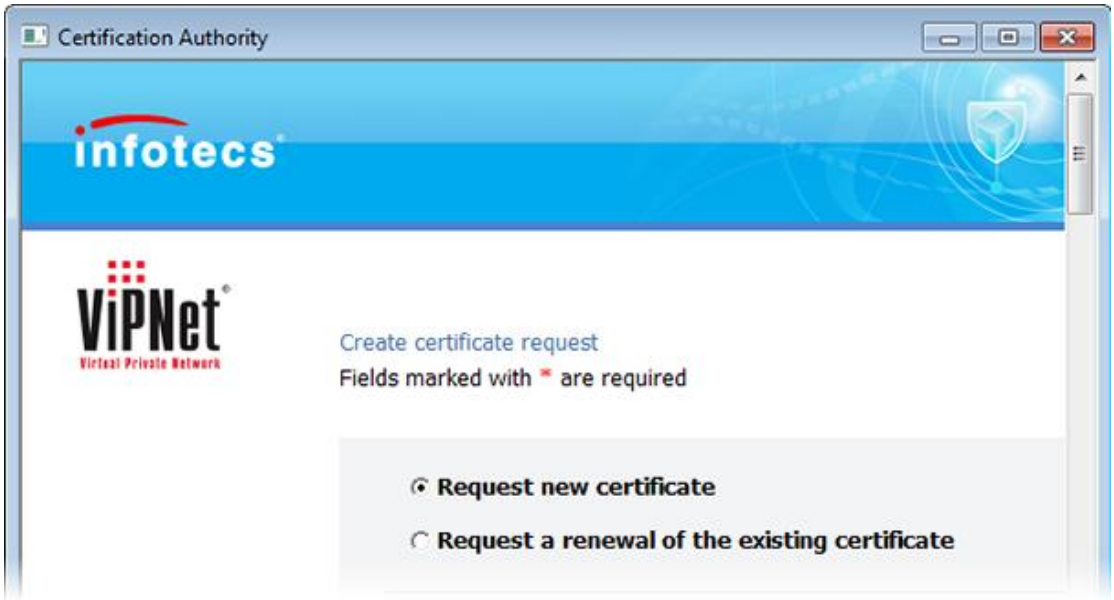

Figure 20: Allowing blocked content

3 In the **Choose Certificate Settings** section, specify the following parameters:

- In the **Cryptoprovider** list, select the cryptographic service provider that you want to use for creating private and public keys.
- In the corresponding list, select a hash algorithm.
- In the **Purpose** list, select the actions a certificate will be used for:
  - **Signature and encryption** (by default), if you want to use your digital signature for encrypting messages and signing them.
  - **Signature**, if you want to use your digital signature only for signing messages or documents.
  - **Encryption**, if you want only to encrypt messages or documents.
- In the **Certificate template** list, choose one of the following options:
  - **Qualified ViPNet CSP** (by default), to create a request for a qualified certificate, in which you may specify OGRNIP (Primary State Registration Number of the Sole Proprietor), SNILS (Insurance Number of Individual Ledger Account), INN (taxpayer identification number), and OGRN (primary state registration number) attributes.
  - **Reporting**, to create a certificate for signing documents intended for submission of financial statements.
  - **WEB server**, to create a certificate on the IIS web server.
  - **Standard** for the remaining cases.
- To have an opportunity to export a certificate, select the **Exportable** check box.
- To create a certificate for installing it to the system store, select the **System** check box.

4 In the **Provide details about the owner of the certificate** section, specify the necessary information about yourself (the person for whom the certificate will be generated).

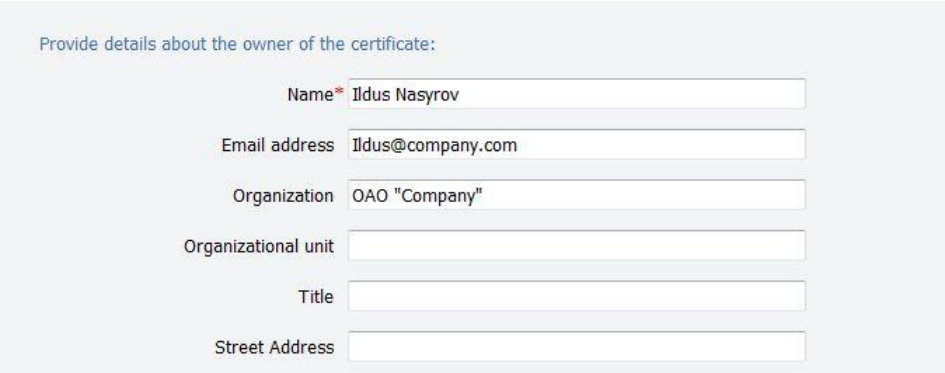

Figure 21: Typing the data on the certificate owner

Warning: If you plan to use the certificate for signing MS Outlook messages, you need to specify the email address.You can't use a certificate without an email address for signing email messages.

5 In the **Save Your Request** section, click **Browse** and specify a folder on a hard or removable drive for storing the request file, and also specify a name for the file.

Note: The request file format is determined by the rules of your Certification Authority. We recommend you to include your name and surname in the request file name so that your request was easily identifiable.

6 Click **Create request**

. This button appears after all required fields are filled.

Warning: If the **Create request** button is not displayed after you fill in all required fields, make sure that, in the **General** section (see figure on page 32), the **Allow ViPNet CSP to use MS Crypto API** check box is selected.

Then, create a key container by performing the following actions.

7 In the displayed **ViPNet CSP — Key Container Initialization** window, specify:

- A container name, or leave the default value.
- The container location by clicking one of the following options: **Folder** or **Choose device**.

Note: In some cases, the **ViPNet CSP — Key Container Initialization** window can be displayed with a delay. Wait until it is displayed.

8 In the **ViPNet CSP — Key Container Initialization** window, specify the private key protection password.

9 The **Digital Roulette** (on page 178) window will be displayed. Follow the instructions in the **Digital Roulette** window.

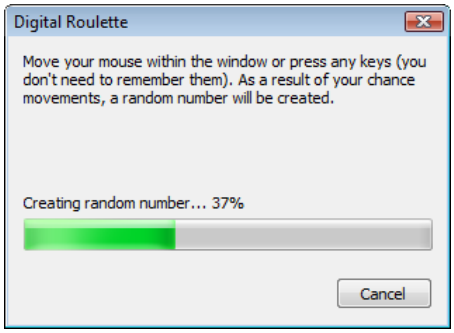
Digital Roulette
Move your mouse within the window or press any keys (you don't need to remember them). As a result of your chance movements, a random number will be created.
Creating random number... 37%
Cancel

Figure 22: Digital Roulette

10 In the message about the successful creation of the certificate request file, click **OK**.

11 After creating the request file, you can close the **Certification Authority** browser page.

After the certificate request is created, deliver your request file to the administrator of your certification authority and get an issued certificate in return. Then, in the **ViPNet CSP Settings** program, install the issued certificate (see Installing the User Certificate in the System Store on page 68) and specify the key container corresponding to this certificate.

Using Signing Keys of the ViPNet Host's User

You can transfer the key container installed on your ViPNet host using the ViPNet CryptoService, ViPNet Client or ViPNet Coordinator program (version 3.2.2 or later), to another computer and use this key container in the ViPNet CSP program.

To use the signature keys of the ViPNet host's user in the ViPNet CSP program, do the following:

1. In the ViPNet CryptoService, ViPNet Client of ViPNet Coordinator, open the **Security Service Settings** dialog box, click the **Keys** tab.
2. Under **Signature**, click **Transfer**.

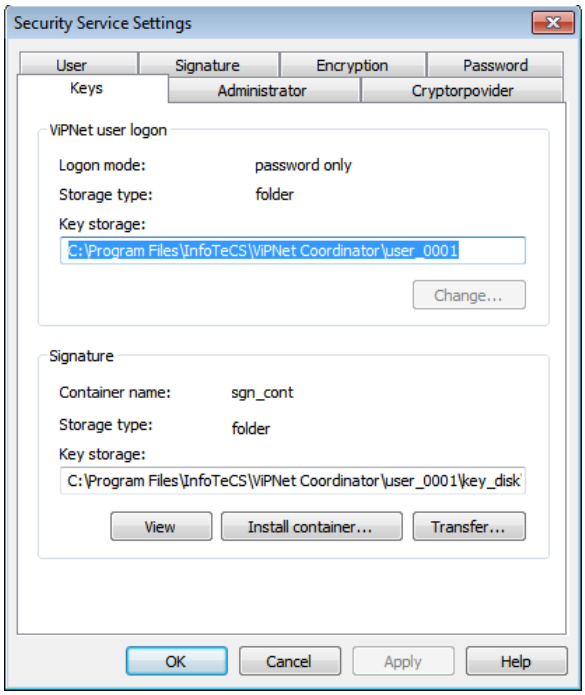

Figure 23: Transferring the key container

3. In the **ViPNet CSP- Key Container Initialization** window, click **Browse** and specify a folder or removable device for transferring the container. Then click **OK**. The container will be transferred into the specified folder.
4. Copy the container to the computer where the ViPNet CSP program installed.

Warning: After you delete the container from your ViPNet host, you can't use signature keys.

5 Install the container in the ViPNet CSP program (see Installing Container from a Folder on page 61).

6

Installing Containers and Certificates

Ways to Install a Private Key and a Certificate	60
Installing Container from a Folder	61
Installing Container from an External Device	64
Installing Certificates in a Container	66
Installing the User Certificate in the System Store	68
Installing Issuer's Certificates and CRL	73

Ways to Install a Private Key and a Certificate

To work with the digital signature, do the following:

1. Install the container containing your private key:
   - If a private key and a certificate are located in the same container in a folder on the hard drive, see the section Installing Container from a Folder (on page 61).
   - If a private key and a certificate are located in the same container on an external device, see the section Installing Container from an External Device (on page 64).
   - If the certificate was issued in the certification authority by request, and as a result you have a container with a private key and a separate cer-file, see the section Installing Certificates in a Container (on page 66).
2. Install a certificate with a public key in the system store (see Installing the User Certificate in the System Store on page 68).
3. Install the issuer's certificate and CRL in the system store (see Installing Issuer's Certificates and CRL on page 73).

Installing Container from a Folder

To work with protected documents and to organize connections over the TLS/SSL protocol, you need a private key and a corresponding certificate. You can install a private key and a certificate in the same container or install a certificate and a container with a private key separately (see Installing the User Certificate in the System Store on page 68).

To install the container, located in a folder on the hard drive, in the system store:

1 In the main **ViPNet CSP** window, select **Containers**.

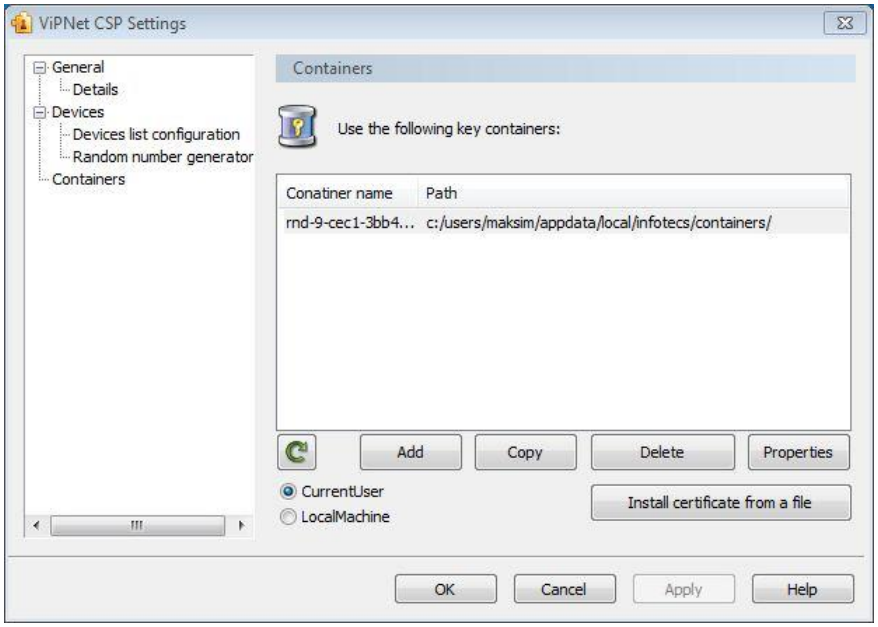

Figure 24: Containers control panel

2 In the **Containers** section, click **Add**.

3 In the **ViPNet CSP - Key Container Initialization** window, click **Browse**.

- If a container is stored on the hard drive, in the **Browse for Folder** window, specify the location of the container.
- If a container is stored on a removable flash-drive, in the **Browse for Folder** window, select this drive. In the **Folder**box, the path will be automatically substituted, for example `E:\infotecs\Containers`.

Warning: On a removable flash-drive, the container should be located in the folder `Infotecs\Containers`.

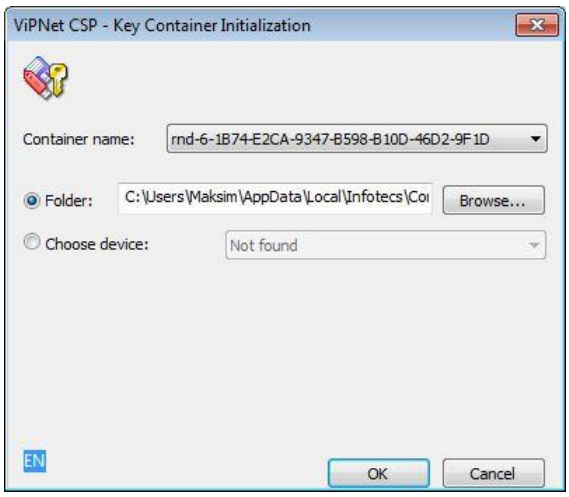

Figure 25: Installing the key container from the folder

4 In the **Container name** list, choose the container file or leave the default value.

5 Click **OK**. In the **Key container** window, a message about the successful container addition will be displayed and you will be prompted to install the certificate in the store. To use certificates, you should install them in the system store of the current user.

Warning: If the ViPNet CSP program is installed on a server and is used to organize connections over the TLS/SSL protocols, you should install your certificate in the local computer's store (see Installing a Certificate from Container on page 71) manually.

If you want to install the certificates automatically in the user's store, click **Yes**. Certificates will be automatically installed in the user's store.

If you don't need to install certificates (or you will install it manually), click **No**.

To view the container's certificate list, click **Certificates**.

6 After you have installed the certificates in a store (or after you have canceled the certificates' installation), in the available containers list (see figure on page 61), the added container will be displayed.

Note: In the certificate settings window, you can install certificates from the container manually (see Installing a Certificate from Container on page 71).

After container adding, install the issuer’s certificate and CRL (see Installing Issuer's Certificates and CRL on page 73) and proceed using cryptographic operations (see ViPNet CSP Scope on page 22).

Installing Container from an External Device

To install container from an external device:

1. In the main **ViPNet CSP** window, select the **Containers** (see figure on page 61) section.
2. In the **Containers** section, click **Add**.
3. In the **ViPNet CSP - Key Container Initialization** window, click **Device**. In the devices list, select the required device.

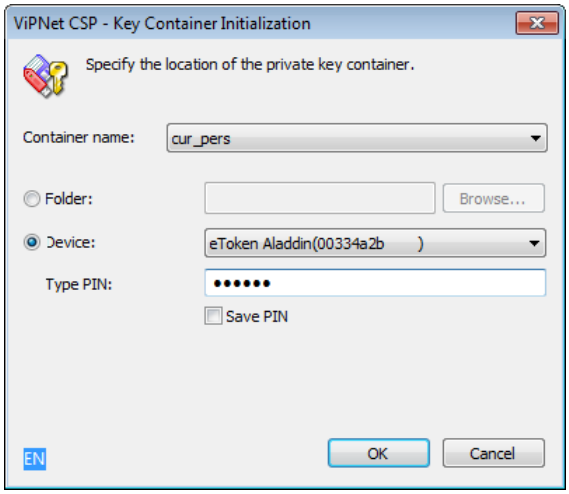

Figure 26: The key container initialization from an external device

4. In the **Type PIN** box, specify the PIN of the selected external storage device. Select the **Save PIN** check box if you don't want to enter PIN every time you connect the container.

> **Note:** If you save PIN of the device in the system, the security level becomes lower.
>
> For more information,see the Supported External Storage Devices (on page 175).

5. Click **OK**. In the **Key container** (see figure on page **Ошибка! Закладка не определена.**) window, the message about successful container addition will be displayed, and you will be prompted to install the certificate in the store. To use certificates, you should install them in the system store of the current user.

If you want to install the certificates automatically in the user's store, click **Yes**. Certificates will be automatically installed in the store.

If you don't need to install the certificates (or you will install them manually), click **No**.

To view the container's certificate list, click **Certificates**.

6 After you have installed the certificates in a store (or after you have canceled the certificates' installation), in the available containers list (see figure on page 61), the added container will be displayed.

Note: You can install certificates from container manually, using certificate settings window (see Installing a Certificate from Container on page 71).

After you have added the container, install the issuer's certificate and CRL (see Installing Issuer's Certificates and CRL on page 73), and then proceed using cryptographic functions (see ViPNet CSP Scope on page 22).

Tip: If an external device has been removed, and then connected to the computer again, the container, which is located on this device, may not appear in the **Containers** section. To display this container in the **Containers section**, click .

Installing Certificates in a Container

When you create a certificate request, the container with a private key is generated. By request, in the Certification Authority, the public key certificate corresponding to this private key is issued.

To use a certificate public key received from the Certification Authority, to generate a digital signature and for other purposes, this certificate should be installed in the container where the corresponding private key is stored.

To install the certificate in a container:

1. In the main **ViPNet CSP** window, select the **Containers** (see figure on page 61) section.
2. In the **Containers** section, choose the container in which you need to install the certificate, and click **Properties** or double-click the necessary container.
3. In the **Key Container Properties** window, click **Add**.

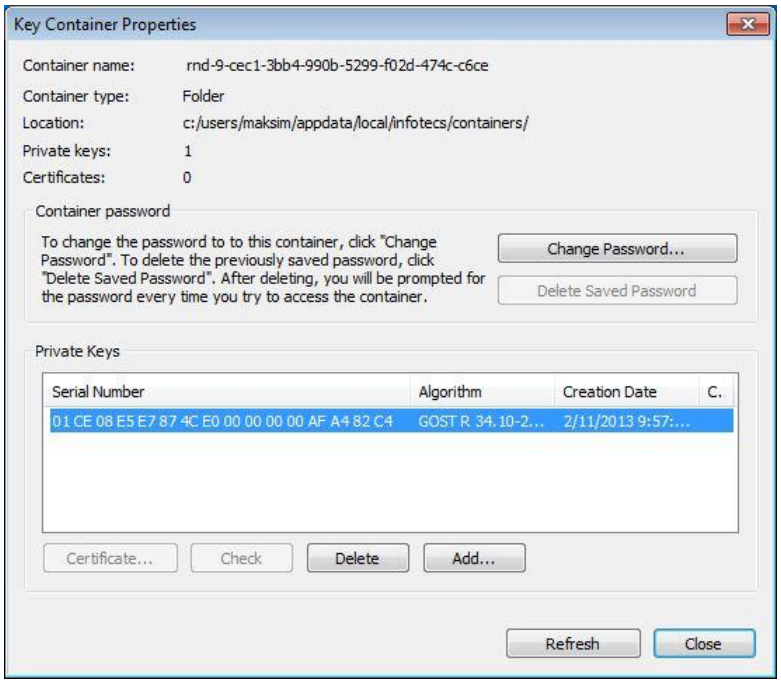
Key Container Properties
Container name: rnd-9-cec1-3bb4-990b-5299-f02d-474c-c6ce
Container type: Folder
Location: c:/users/maksim/appdata/local/infotecs/containers/
Private keys: 1
Certificates: 0
Container password
To change the password to to this container, click "Change Password". To delete the previously saved password, click "Delete Saved Password". After deleting, you will be prompted for the password every time you try to access the container.
Change Password...
Delete Saved Password
Private Keys
Serial Number
Algorithm
Creation Date
C.
01 CE 08 E5 E7 87 4C E0 00 00 00 00 AF A4 82 C4
GOST R 34.10-2...
2/11/2013 9:57:...
Certificate...
Check
Delete
Add...
Refresh
Close

Figure 27: Adding the certificate to the container

4. In the **Open** window, select the certificate file, which corresponds to the private key in the container, and click **Open**. If you have chosen the correct certificate, it will be added to the container. Otherwise, you will see an Invalid certificate message.

Note: To view this certificate after adding, in the **Key Container Properties** window, click **Refresh**.

Installing the User Certificate in the System Store

To use a public key certificate in different applications, you should install it in the certificates system store. There are two ways to do it:

- If the certificate is not installed in the container with the corresponding private key, you should install the certificate in the system store in the Containers (see Installing a Certificate Which Has Not Been Added to the Container on page 68) section.
- If the certificate is already installed in the container, you should install the certificate in the system store in the viewing certificate window (see Installing a Certificate from Container on page 71).

Installing a Certificate Which Has Not Been Added to the Container

If the certificate is not added to the container, to install the certificate in the system store, do the following:

1. In the main ViPNet CSP window, select the **Containers** (see figure on page 61) section.
2. In the **Containers** section, click **Install certificate from a file**.
3. In the **Open** window, specify the path to the certificate file on a disk (see Key Container on page 18).
4. In the certificates installation wizard, on the start page, click **Next**.
5. On the **Choose the certificate store** page, specify the store to install you certificate in and click **Next**.

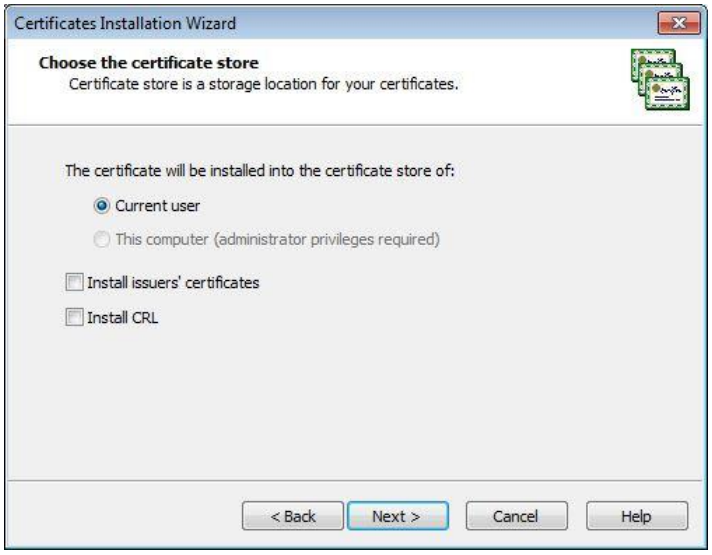
Certificates Installation Wizard
Choose the certificate store
Certificate store is a storage location for your certificates.
The certificate will be installed into the certificate store of:
Current user
This computer (administrator privileges required)
Install issuers' certificates
Install CRL
< Back
Next >
Cancel
Help

Figure 28: Choosing a certificate store

Note: We recommend you to install a certificate into the store of the current user in order to encrypt, decrypt, and sign files, as well as to get access to protected resources using a web browser. In the machine computer's store, install the certificates that will be used by services on this computer.

If you use ViPNet CSP on a web server to get access to protected resources, you need to install a certificate into the store.

If you can't install a certificate into the store, log onto the system as an administrator.

---

6 On the **Ready to install this certificate** page:

- Check if the parameters have been configured correctly. If necessary, click **Back** to return to the previous page of the wizard and configure the parameters in a different way.

Certificates Installation Wizard
Ready to install this certificate
The wizard is ready to install this certificate to the system store.
You have specified the following settings:
Certificate store selected
Current user
Additional options
Don't install issuers' certificates.
Don't install certificate revocation list.
You can choose the container with your private key. Information about this container will be added to the certificate store.
Choose container with your private key
< Back
Next >
Cancel
Help

Figure 29: The certificate is ready for installation

- If the certificate is stored in a file separately from the private key, select the **Choose container with your private key** check box.

Note: The **Choose container with your private key** check box is optional. If you do not select the check box, , after the wizard completes the operation, you will need to specify the private key container location.

- Click **Next**.

7 If the **Choose container with your private key** check box is selected and the container is not found or is unavailable, then, in the **ViPNet CSP — Key Container Initialization** window, specify the key container location:

- a folder on a disk (see Installing Container from a Folder on page 61);
- a device (you will need to specify its parameters and a PIN (see Installing Container from an External Device on page 64)).

Note: To use an external device, you need to connect it and install the required drivers. You can find the list of compatible storage devices and basic information on how to use them in Supported External Storage Devices (on page 175).

Then click **OK**.

8 In the “Do you want to store both the certificate and the private key in the same container?” message window, click **Yes** to store the certificate in the key container, or **No** to keep the certificate as a separate file.

Tip: It is convenient to store a certificate in a key container if you are going to export and install the container onto another computer.

9 If the **Choose container with your private key** check box is selected and the container is available, in the **ViPNet CSP — Key Container Password** window, in the **Password** box, type the password to access the container and click **OK**.

Note: The **ViPNet CSP — Key Container Password** window is not displayed if you have previously saved the password and selected the **Do not show this window again** check box.

10 On the **Completing the Certificates Installation Wizard** page, click **Finish**.

As a result, the certificate is installed into the selected certificate store. In case no private key has been found when installing the certificate, you should install the key container corresponding to this certificate.

If during installation the certificate was associated with the private key, the container with the private key corresponding to this certificate appears on the list of containers (see figure on page 61) (see the figure on page). You may install one more certificate and private key or begin working with protected documents (see ViPNet CSP Scope on page 22) using the previously installed issuer’s certificate and CRL (see Installing Issuer's Certificates and CRL on page 73).

Installing a Certificate from Container

To install certificate:

1 In the main **ViPNet CSP** window, select the **Containers** (see figure on page 61) section.

2 In the **Containers** section, choose the container, whose you need to install the certificate, and click **Properties** or double-click the necessary container.

3 In the **Key Container Properties** (see figure on page 77) window, choose a necessary private key and click **Certificate**.

4 In the **Certificate** window, on the **General** tab, click **Install Certificate**. The Certificate Renewal Wizard (see Installing the User Certificate in the System Store on page 68) window will be displayed.

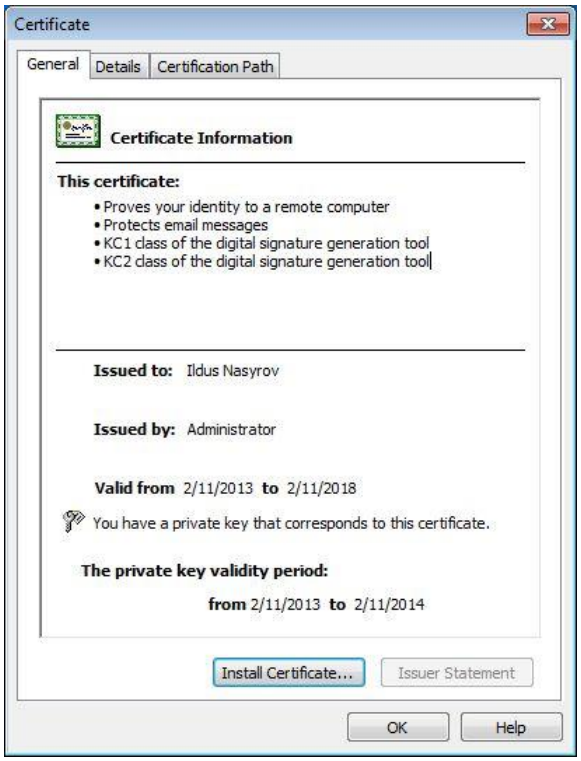

Figure 30: Viewing the certificate properties

5 In the **Certificates Installation Wizard**, on the start page, click **Next**.

6 On the **Choose the certificate store** page, specify the necessary store.

7 On the **Ready to install this certificate** page, clear the **Choose the container with your private key** check box, and click **Next**.

8 On the **Completing the Certificates Installation Wizard** page, click **Finish**. As a result, the certificate will be installed into the store.

To work with protected documents and to organize connections over the TLS/SSL protocol, you need to install not only the user's certificate, but also the issuer's certificate and CRL (see Installing Issuer's Certificates and CRL on page 73).

Installing Issuer's Certificates and CRL

To work with protected documents and to organize connections over the TLS/SSL protocol, you need to install the user's certificate, the issuer's certificate, and the CRL in the system store. To install the user's certificate in a container or separately, use the ViPNet CSP program means.

You can install the issuer's certificate and CRL by using the operating system tools. Such a type of installing the certificate is also required if the ViPNet software is installed on a web server and used to organize connections over TLS/SSL.

To install certificates and CRL:

1. Open the folder, containing the certificate file or CRL. Right-click the necessary file and, on the context menu, select **Install Certificate** or **Install CRL**.
2. On the start page of the Certificate Import Wizard, click **Next**.
3. On the **Certificate store** page, select **Place all certificates in the following store**.

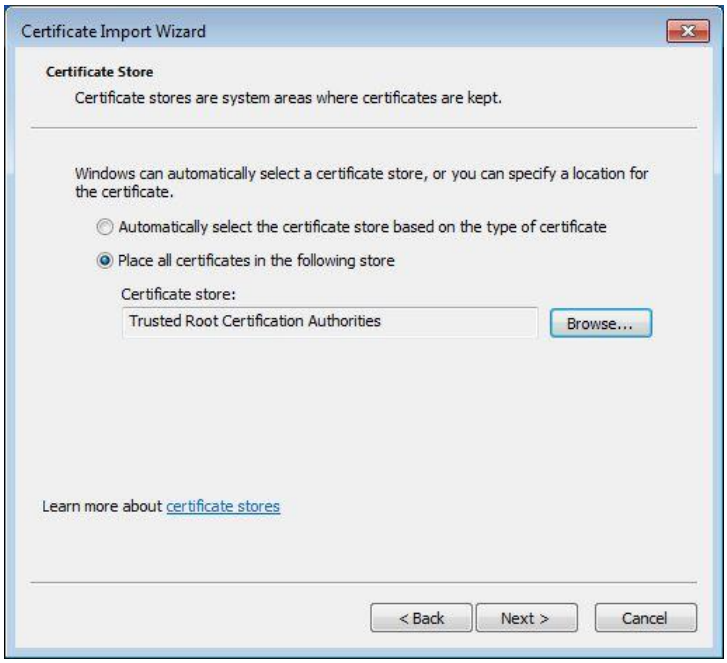
Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Trusted Root Certification Authorities
Browse...
Learn more about certificate stores
< Back
Next >
Cancel

Figure 31: Choosing a store for the issuer's certificate or CRL

4. Click **Browse**. In the **Select Certificate Store** window, select:
   - **Trusted Root Certification Authorities**, if you are installing an issuer's certificate.

- **Intermediate Certification Authorities**, if you are installing CRL.

Click **OK**.

5 After you choose a certification store, click **Next**.

6 On the **Completing the Certificate Import Wizard** page, click **Finish**.

Warning: If the system can't validate the certificate (for example, if the Internet connection or ViPNet host is not available), then the **Security Warning** window will be displayed. To install the certificate, click **Yes**.

Install only the certificates, in which you are confident.

7 In the "The import was successful" message box, click **OK**. The installation will be complete.

After that, if you have already installed the user's certificate, you may begin working with protected documents (see ViPNet CSP Scope on page 22).

7

Working with Containers

Viewing and Configuring Container Properties	76
Creating a Backup Copy of a Container	81
Deleting a Container	82

Viewing and Configuring Container Properties

In the container properties window you may:

- View information about a private key and a certificate, which are stored in the container.
- Change the password you use to access a container.
- Delete a previously saved container password.
- Install a certificate manually.
- Check or delete a private key stored in a container.

Changing the Container Password

To change the password of the container, which is located in a folder on the disk:

1. In the main **ViPNet CSP** window, select the **Containers** (see figure on page 61) section.
2. To select a key container from the current user's key containers folder, click **Current user**. To select a key container from the computer's key containers folder, click **Computer**.
3. Select a key container, whose you need to change password, and click **Properties** or double-click the necessary container.
4. In the **Container Properties** window, click **Change Password**.

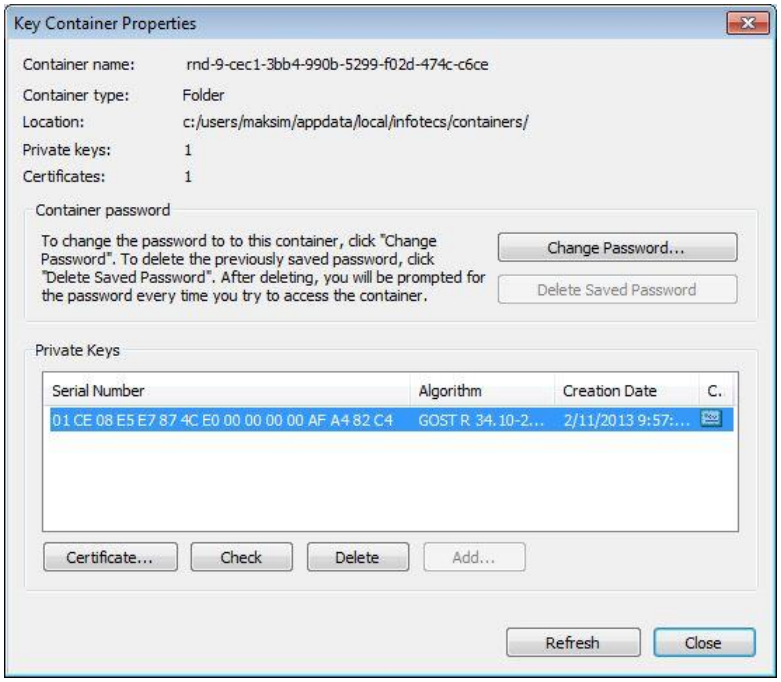
Key Container Properties
Container name: rnd-9-cec1-3bb4-990b-5299-f02d-474c-c6ce
Container type: Folder
Location: c:/users/maksim/appdata/local/infotecs/containers/
Private keys: 1
Certificates: 1
Container password
To change the password to to this container, click "Change Password". To delete the previously saved password, click "Delete Saved Password". After deleting, you will be prompted for the password every time you try to access the container.
Change Password...
Delete Saved Password
Private Keys
Serial Number
Algorithm
Creation Date
C.
01 CE 08 E5 E7 87 4C E0 00 00 00 00 AF A4 82 C4
GOST R 34.10-2...
2/11/2013 9:57:...
Certificate...
Check
Delete
Add...
Refresh
Close

Figure 32: Container properties window

5 In the **Change password** dialog box, type the current container password, then click **OK**.

Note: If you have previously selected the **Save password** check box, then the **Change Password** window will not be displayed.

6 In the **ViPNet CSP — Key Container Password** window, type the new password and confirm it. Click **OK**.

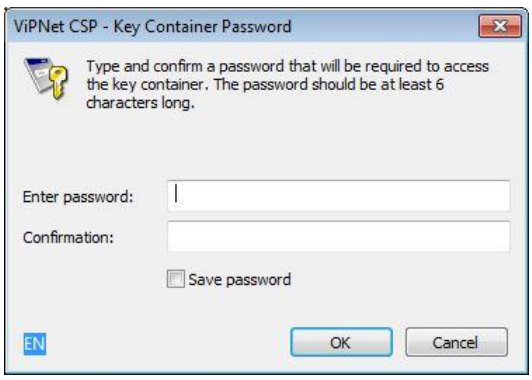
ViPNet CSP - Key Container Password
Type and confirm a password that will be required to access the key container. The password should be at least 6 characters long.
Enter password:
Confirmation:
Save password
EN
OK
Cancel

Figure 33: Changing the container password

The container password is changed.

Deleting a Previously Saved Password

You may need to delete the saved password to a key container in case the password storage conditions and (or) you corporate security regulations have changed so that you may not store the password on your computer anymore.

To delete a previously saved container password:

1. In the main **ViPNet CSP** window, select the **Containers** (see figure on page 61) section.
2. To select a key container from the current user's key containers folder, click **Current user**. To select a key container from the computer's key containers folder, click **Computer**.
3. Select a key container, whose you need to delete password, and click **Properties** or double-click the necessary container.
4. In the **Key Container Properties** (see figure on page 77) window, click **Delete Saved Password**. The password will be deleted.

The previously saved password will be removed. Then you should enter the password every time you access the key container.

Verifying a Key Container

You can verify a key container to make sure that the container file has not been modified, that the certificate and private key in the container correspond to each other and you can use them to work with protected documents.

To verify a container:

1. In the **Container Properties** window (see figure on page 77), in the **Private Keys** list, choose the private key entry.
2. Click **Check**.
3. In the **ViPNet CSP — Key Container Password** window (see figure on page 79) type the password to access the container and click **OK**.

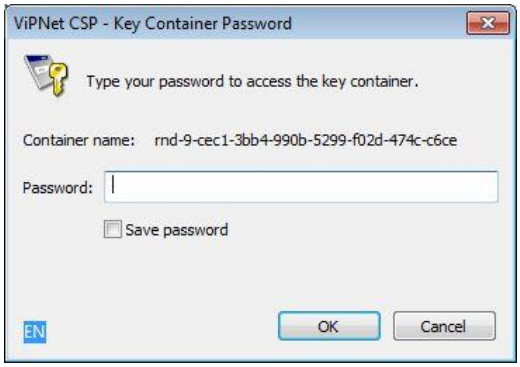

Figure 34: Typing the container password

4 Then the data fragment signed with the private key will be created, and the digital signature will be verified using the public key certificate. Thus, the private key validity and its compatibility with the certificate stored in the container will be verified.

Note: You can verify a key container only if it contains a certificate corresponding to the private key. A certificate may be missing from a key container, when it is stored separately. A certificate is stored separately from a key container if the certificate renewal request has been generated in the ViPNet CSP software. If the renewal request has been generated in another program, the certificate will be automatically saved to the corresponding key container.

When the private key is verified, the certificate validity (its validity period, presence in CRL, and so on) **is not verified**.

Deleting a Private Key

It is required to delete the private key (and, if present, its certificate) from the container key in the following cases:

- If you don't need this private key any more, for example, if its validity period has expired.
- If the certificate corresponding to this private key has been compromised or revoked.

To delete a private key from a container:

1 In the **Container Properties** (see figure on page 77) window, in the **Private Keys** list, choose the private key entry or several entries holding the **Shift** key.

2 Click **Delete**. You will receive a warning message that you will not be able to restore the deleted private keys.

3 Confirm the operation by clicking **Yes**.

The private key you have chosen and the corresponding certificate will be deleted. You should delete the key container after that.

Creating a Backup Copy of a Container

You can transfer a key container to a folder on a hard drive or to an external device. This function is useful for creating backup copy of key container and for increasing the data protection level.

To copy container:

1. In the main **ViPNet CSP** window, select the **Containers** (see figure on page 61) section.
2. To select a key container from the current user's key containers folder, click **Current user**. To select a key container from the computer's key containers folder, click **Computer**.
3. Select container that you want to copy and click **Copy**.
4. In the **ViPNet CSP - Key Container Initialization** (see figure on page 77) window, specify and confirm a password, which will be used to access created backup copy.
5. In the **ViPNet CSP - Key Container Initialization** window, specify a new container name and location. You can copy a key container to a folder on a hard drive or to an external device.
6. In the **ViPNet CSP - Key Container Initialization** (see figure on page 79) window, type password (or PIN, if container located on the external device) to access container, which you need to copy.

   To save password for next reference to container, select the **Save password** check box.

   Note: If you save PIN of the device in the system, the security level becomes lower.

7. The container copy will be displayed in the specified folder (or on an external device).

Deleting a Container

If you don't want to use some certificate or a private key, you may delete the corresponding container. To do this:

1. In the main **ViPNet CSP** window, select the **Containers** (see figure on page 61) section.
2. To select a container from the current user's key containers folder, click **Current user**. To select a container from the computer's key containers folder, click **Computer**.
3. Select a container you want to delete and click **Delete**.

Warning: A deleted container can't be used. We strongly recommend you to create a backup copy of the container (see Creating a Backup Copy of a Container on page 81).

4. To confirm deleting of the container, in the displayed window, click **OK**.

   The container will be deleted from the containers list and also from the folder or from an external device, where it is stored.

8

Managing External Devices

Viewing the Connected Devices List	84
Configuring the Devices List	86
External Device Initialization	87
Changing PIN	88
Using a Random Number Generator	89

Viewing the Connected Devices List

ViPNet CSP allows you to work with key containers, which are stored on an external devices.

To view connected device list and key containers, stored on them:

1 In the main **ViPNet CSP** window, select **Devices** section.

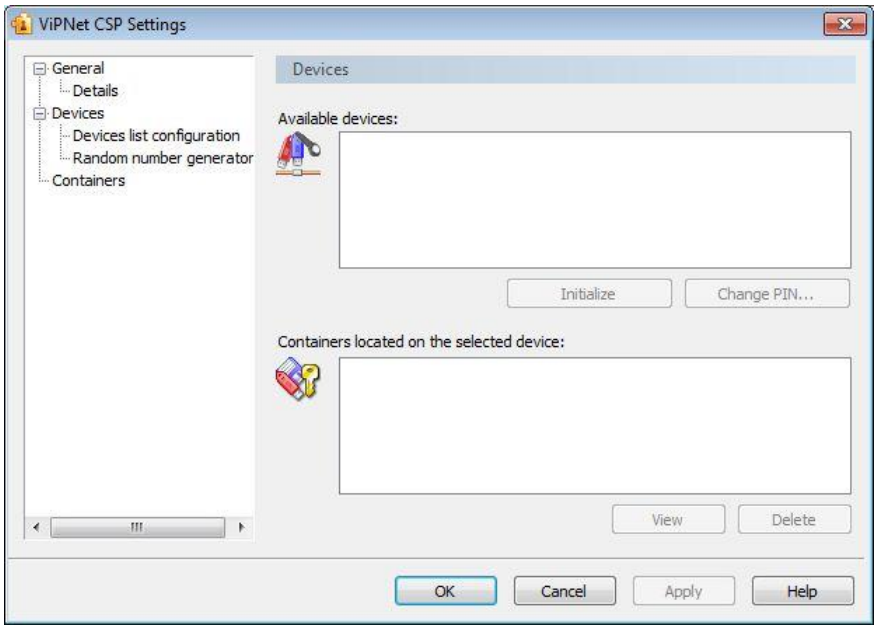

Figure 35: The Devices section

2 In the **Available devices** list, choose necessary device.

Note: In the **Available devices** list, only those devices are displayed, that are connected to the corresponding card reader at the moment.

3 In the **Containers located on the selected device** list, choose a container.

- To view the container properties, click **View** (see Viewing and Configuring Container Properties on page 76).
- To delete the container from an external device, click **Delete**.

Note: If the **Containers located on the selected device** list is empty, there are no containers on this device.

Configuring the Devices List

On the **Devices list configuration** tab, you can specify the types of devices, which should be polled when the search for keys is performed. If the check box associated with a device type is cleared, such devices can't work with the program.

By default, all supported devices are polled. To increase the speed of key search, disable devices you don't use. To do this:

1 In the main **ViPNet CSP** window, select the **Devices list configuration** section.

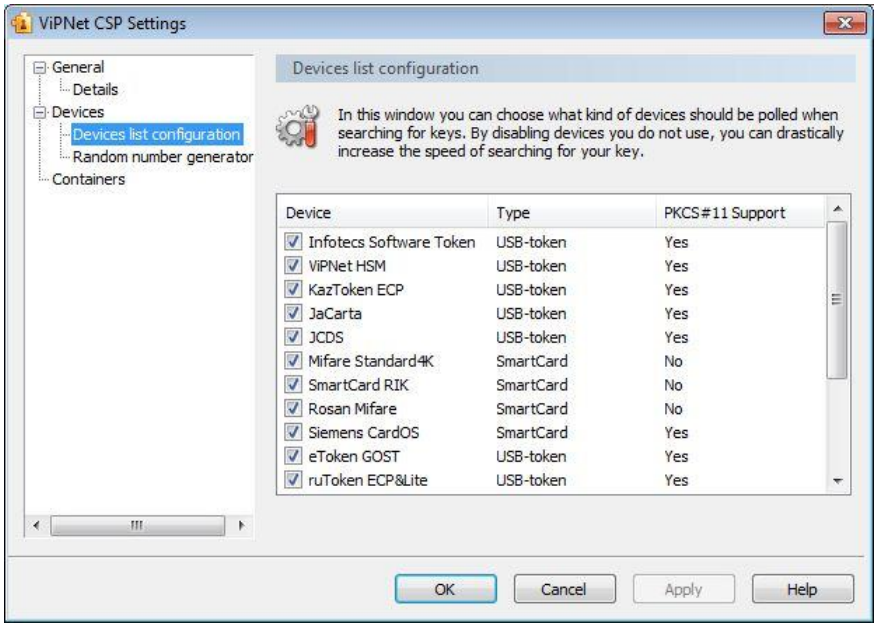

Figure 36: Devices list configuration

2 Clear the check boxes corresponding to the devices, that you don't use.

3 To save the settings, click **Apply**.

External Device Initialization

Initialization means formatting the device memory. During initialization, all data stored on the device are removed. Password and other settings are dumped.

To initialize your connected device:

1. Make sure that the device you are going to initialize does not contain any important information. If necessary, copy the information from the external device to another device or hard drive.
2. In the main **ViPNet CSP** window, select the **Devices** (see figure on page 84) section.
3. Choose a device from the **Available devices** list.

Note: In the **Available devices** list, only those devices are displayed, that are connected to the corresponding card reader at the moment.

4. Click **Initialize**.
5. In the message window warning you about deleting all data from the device, click **Yes**.
6. In the **Initialization** window:
   - Type the device administrator PIN.
   - If necessary, change the user PIN. To do that, type a new PIN and confirm it in the corresponding boxes.
7. Click **OK**.

   The device will be initialized. All data saved on a device will be lost. Now you need to use the new user PIN to access the device.

Changing PIN

Device PIN change may be required when the password expires according to the corporate security policy or by other reasons regulated.

To change the device PIN:

1. In the main **ViPNet CSP** window, select the **Devices** (see figure on page 84) section.
2. Choose a device from the **Available devices** list.

> **Note:** In the **Available devices** list, only those devices are displayed, that are connected to the corresponding card reader at the moment.

3. Click **Change PIN**.
4. In the **Change PIN** window, select the PIN you need to change.
5. In the **Type old PIN** box, type the current PIN. In the other two boxes, type your new PIN and then click **OK**.

PIN will be changed.

Using a Random Number Generator

A random number generator creates a sequence of numbers, based on which private keys are generated.

As a random number generator, in ViPNet CSP, you can use an integrated biological random number generator (Digital Roulette).

To choose random number generator, that you want to use:

1 In the main **ViPNet CSP** window, select the **Random number generator** section.

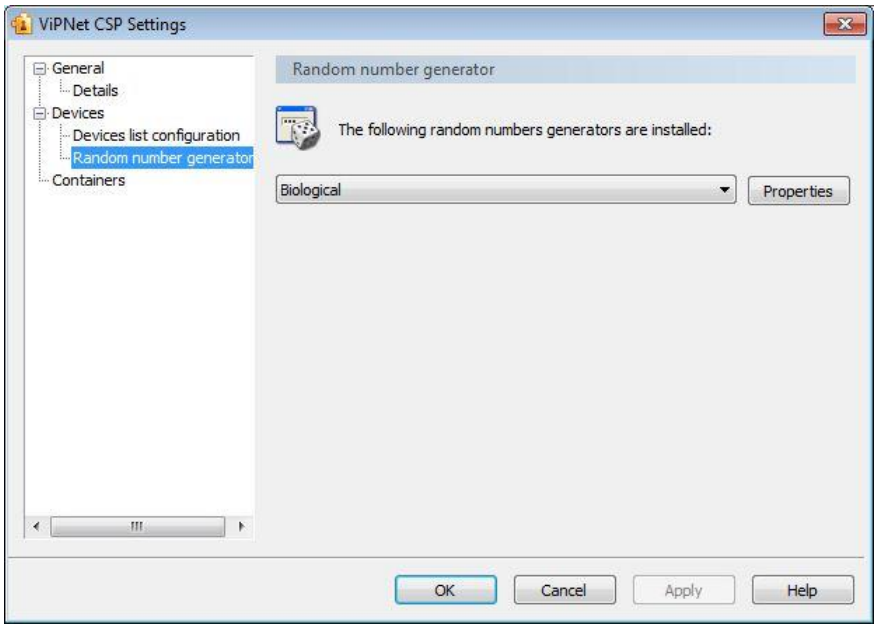

Figure 37: Random number generator tab

2 In the **The following random number generators are installed** list, choose one of the following:

- **Biological**, to use Digital Roulette for generating random numbers.
- **External device (Token) PKCS#11**, to use external devices eToken Aladdin or eToken GOST for generating random numbers.
- **Random binary sequence**, to use a previously generated sequence of numbers. If you choose this option:
  - Click **Properties**.

- In the **Properties** window, click **Add binary sequence**.
- In the **Browse** window, select a folder, where the files containing binary sequence are located.

o Hardware random numbers generator, installed on computer.

3 To save properties, click **OK**.

4 To view information about chosen random number generator, click **Properties**.

To check the operability of biological or hardware random number generators, in the **Properties** dialog box, click **Test**. After the test, the results will be displayed.

Digital Signature in Microsoft Office Documents

Digitally Signing a Document 92

Viewing a Digital Signature 96

Removing a Digital Signature 99

Visible Representation of a Signature Line in Word and Excel Documents 101

Digitally Signing a Document

When you working with documents in Microsoft Office programs, you may use a digital signature.

This section contains information about adding a digital signature in Microsoft Word, Excel and PowerPoint documents of various Microsoft Office versions.

Microsoft Office 2003

To add a digital signature in Microsoft Word, Excel, and PowerPoint documents:

1. Save a document.
2. On the **Tools** menu, click **Options**.
3. On the **Security** tab, click **Digital Signatures**.
4. In the **Digital Signature** window, click **Add**.

Figure 38: Adding a digital signature in Microsoft Office 2003

Note: If you haven't saved the document earlier, you will be prompted to save it before adding a digital signature. In the message window, click **Yes**.

1. The **Select a Certificate** window will be displayed. To view information about certificate, select it and click **View Certificate**.
2. In the **Select a Certificate** window, select the certificate and click **OK**. The **ViPNet CSP — Key Container Password** (see figure on page 79) window will be displayed.
3. Type your password and click **OK**. The chosen certificate will appear in the **The following have digitally signed this document** list in the **Digital Signature** window.
4. Double-click **OK**, to close the windows. On the status bar of the document window, the icon will be displayed. This icon means that the document contains a digital signature.

If you edit a document after it was signed and try to save it, you will be notified that all digital signatures will be removed. If necessary you may sign it again after saving.

Microsoft Office 2007

To add a digital signature in Microsoft Word, Excel, and PowerPoint documents:

1. Click the **Microsoft Office** button, point to **Prepare**, and then click **Add a Digital Signature**. The **Sign** window will be displayed.

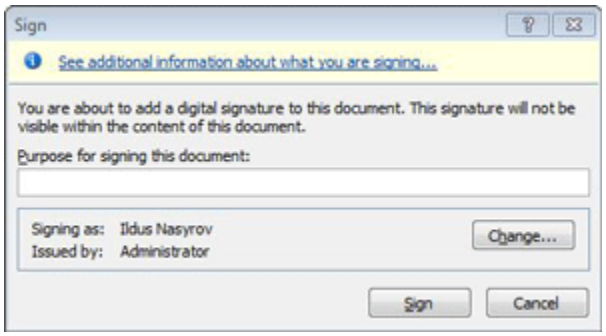
Sign
See additional information about what you are signing...
You are about to add a digital signature to this document. This signature will not be visible within the content of this document.
Purpose for signing this document:
Signing as: Ildus Nasyrov
Issued by: Administrator
Change...
Sign
Cancel

Figure 39: Adding a digital signature in Microsoft Office 2007

Note: If you haven't saved the document earlier, you will be prompted to save it before adding a digital signature. In the message window, click **Yes**.

1. In the **Sign** window, you can fill out the **Purpose for signing this document** box. Also, this window contains brief description of certificate that you use for signing this document. If necessary, click **Change** and choose another certificate.
2. When you have chosen the certificate, click **Sign**. The **ViPNet CSP — Key Container Password** (see figure on page 79) window will be displayed.
3. Type your password and click **OK**. The message about the successful addition of the digital signature and saving a document will be displayed. On the status bar of the document window, the icon will be displayed. This icon means that the document contains a digital signature.

After you have added a digital signature, you can't edit the document. To edit signed document, you need to remove a digital signature (see Removing a Digital Signature on page 99).

Microsoft Office 2010

To add a digital signature in Microsoft Word, Excel and PowerPoint documents:

1. Click the **File** tab, and click the **Info** section.
2. Under **Permissions**, click **Protect Document**, **Protect Workbook** or **Protect Presentation**, and click **Add a Digital Signature**.
3. Read the Microsoft Word, Excel or PowerPoint message, and click **OK**. The **Sign** window will be displayed.

Note: If you haven't saved the document earlier, you will be prompted to save it before adding a digital signature. In the message window, click **Yes**.

---

1. In the **Sign** window, you can fill out the **Purpose for signing this document** box. Also, this window contains brief information about the certificate that you use for signing this document. If necessary, click **Change** and choose another certificate.

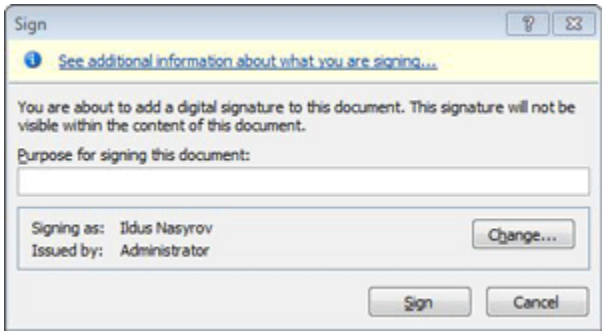
Sign
See additional information about what you are signing...
You are about to add a digital signature to this document. This signature will not be visible within the content of this document.
Purpose for signing this document:
Signing as: Ildus Nasyrov
Issued by: Administrator
Change...
Sign
Cancel

Figure 40: Adding a digital signature in Microsoft Office 2010

2 When you have chosen the certificate, click **Sign**. The **ViPNet CSP — Key Container Password** (see figure on page 79) window will be displayed.

3 Type your password and click **OK**. The message about the successful addition of the digital signature will be displayed.

In the **Info** section, this document will be marked as final to discourage editing.

View Signatures
Signed Document
This document has been signed and marked as final. It should not be edited. If anyone tampers with this document, the signatures will become invalid.
Protect Document
Permissions
This document has been marked as final to discourage editing.

Figure 41: The document has been marked as final to discourage editing

On the status bar of the document window, the icon will be displayed. This icon means that the document contains a digital signature.

After you have added a digital signature, you can't edit the document. To edit the signed document, you need to remove a digital signature (see Removing a Digital Signature on page 99).

Viewing a Digital Signature

Microsoft Office 2003

To view a digital signature in Microsoft Word, Excel or PowerPoint document:

1. On the **Tools** menu, click **Options**.
2. On the **Security** tab, click **Digital Signatures**.
3. In the **Digital Signature** window, choose a certificate and click **View Certificate** (see figure on page 92).

   If the certificate is not trusted, on the **General** tab of the **Certificate** window, the message (see figure on page 96) will be displayed. The untrusted certificate is marked with a red X.

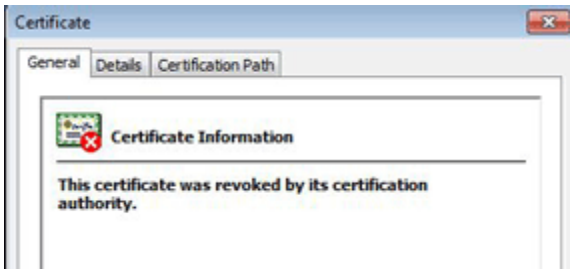

Figure 42: A revoked certificate

Microsoft Office 2007

Warning: The documents signed in Microsoft Office 2010 or 2013 programs can't be correctly recognized in Microsoft Office 2007 programs of the builds earlier than 12.0.6554. We recommend you not to use the earlier builds.

To view a digital signature in Microsoft Word, Excel, or PowerPoint document:

1. Click the **Microsoft Office** button, point to **Prepare**, and then click **View Signatures**. The **Signatures** (see figure on page 97) pane will be displayed.

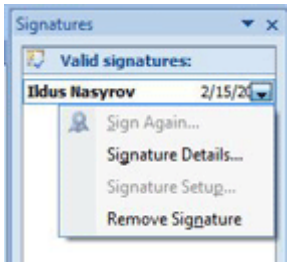

Figure 43: Viewing your digital signatures in Microsoft Office 2007

Note: Moreover, you may open the **Signatures** pane by clicking the digital signature icon on the status bar.

2 On the **Signatures** pane, right-click the signature string and click **Signature Details**.

3 The **Signature Details** (see figure on page 98) window contains brief information about the signature and the certificate. In this window, you may perform the following tasks:

- To open a certificate, click **View**.
- To view the additional signing information, click the **See the additional signing information that was collected** link.

If any certificate validation errors occur, the corresponding message will be displayed under the window title.

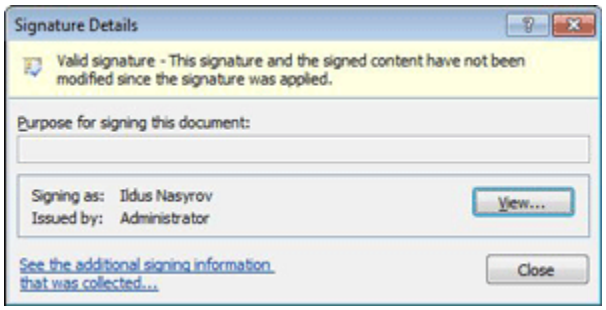
Signature Details
Valid signature - This signature and the signed content have not been modified since the signature was applied.
Purpose for signing this document:
Signing as: Ildus Nasyrov
Issued by: Administrator
View...
See the additional signing information that was collected...
Close

Figure 44: Signature details

Microsoft Office 2010

Warning: Documents that were signed in Microsoft Office 2003 or Microsoft Office 2007 programs can't be open in Microsoft Office 2010 up to build 14.0.6023. We recommend you to use this build or later builds.

To view a digital signature in Microsoft Word, Excel or PowerPoint document:

1 Click the **File** tab and, in the **Info** section, click **View signatures**. The **Signatures** pane will be displayed.

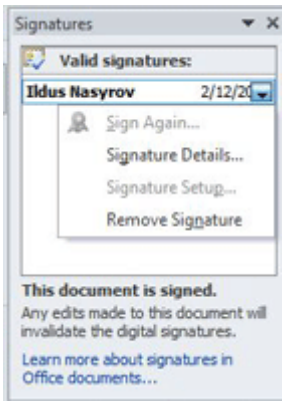

Figure 45: Viewing your digital signatures in Microsoft Office 2010

Note: Moreover, you may open the **Signatures** pane by clicking the digital signature icon on the status bar.

2 On the **Signatures** pane, right-click the signature string and click Signature Details. On the menu, click **Signature Details**.

3 The **Signature Details** (see figure on page 98) window contains brief information about the signature and the certificate. If any certificate validation errors occur, the corresponding message will be displayed under the window title.

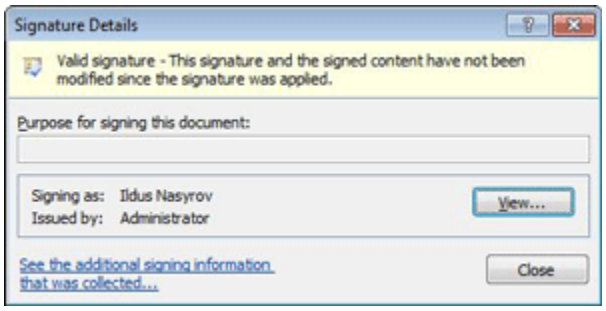
Signature Details
Valid signature - This signature and the signed content have not been modified since the signature was applied.
Purpose for signing this document:
Signing as: Ildus Nasyrov
Issued by: Administrator
View...
See the additional signing information that was collected...
Close

Figure 46: Signature details

4 To open a certificate, click **View**. To view the additional signing information, click the **See the additional signing information that was collected** link.

Removing a Digital Signature

Microsoft Office 2003

To remove a digital signature from a Microsoft Word, Excel or PowerPoint document:

1. On the **Tools** menu, click **Options**.
2. On the **Security** tab, click **Digital Signatures**.
3. In the **Digital Signature** (see figure on page 92) window, choose a certificate to remove. To view the signing certificate, click **View Certificate**.
4. After choosing a digital signature, click **Remove**. The digital signature will be removed.

Microsoft Office 2007

To remove a digital signature from a Microsoft Word, Excel or PowerPoint document:

1. Open the **Signatures** pane by doing one of the following:
   - Click **Microsoft Office** button, click **Prepare**, and then click **View Signatures**.
   - Click the digital signature icon on the status bar of the document.
2. On the **Signatures** pane (see figure on page 97), move the mouse cursor on a signature string and right-click it (or click the menu button on the right), and choose **Remove signature**.
3. To confirm the operation, click **Yes**. The digital signature will be removed from the document.

Microsoft Office 2010

To remove a digital signature from a Microsoft Word, Excel or PowerPoint document:

1. Open the **Signatures** pane by doing one of the following:
   - Click the **File** tab and, in the **Info** section, click **View signatures**.
   - Click the digital signature icon on the status bar of the document.

2 On the **Signatures** pane (see figure on page 97), move the mouse cursor on a signature string and right-click it (or click the menu button on the right), and choose **Remove signature**.

3 To confirm the operation, click **Yes**. The digital signature will be removed from the document.

Visible Representation of a Signature Line in Word and Excel Documents

You can add a visible representation of a signature line in the Microsoft Office software of 2007 and 2010 versions. A signature line resembles a typical signature placeholder that might appear in a printed document. When a signature line is inserted into an Office file, the author can specify information about the intended signer. When an electronic copy of the file is sent to the intended signer, this person sees the signature line and a notification that their signature is requested.

Adding a Signature Line to a Document

To add a signature line to a document:

1. Place your pointer where you want to create a signature line.
2. On the **Insert** tab, under the **Text** group, click **Signature line**. The **Signature Setup** window will be displayed.

Signature Setup
Suggested signer (for example, John Doe):
Suggested signer's title (for example, Manager):
Suggested signer's e-mail address:
Instructions to the signer:
Before signing this document, verify that the content you are signing is correct.
Allow the signer to add comments in the Sign dialog
Show sign date in signature line
OK
Cancel

Figure 47: Signature setup

3. Fill in the following boxes: **Suggested signer**, **Suggested signer's title**, and **Suggested signer's e-mail address**. You may add short instructions for the signer, allow the signer to type the purpose for signing and enable date displaying. You can do it by selecting the corresponding check boxes.
4. After you complete the signature setup, click **OK**. An empty signature line will be inserted in your document and also will be displayed on the **Signatures** pane.

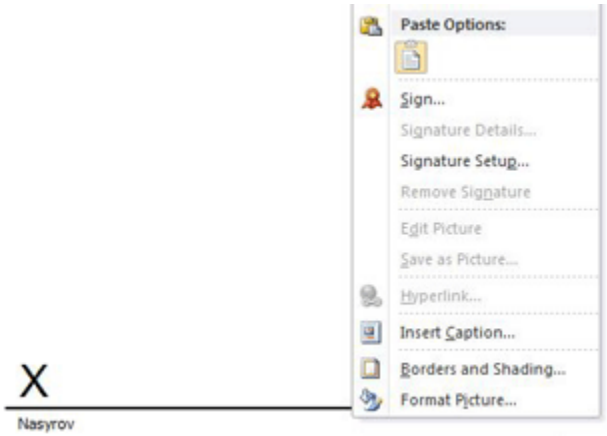

Figure 48: A visible signature line and its representation in the interface

Before you add a digital signature to a signature line, you can change the signature settings. To do this:

1. Depending on the MS Office software version, do one of the following:
   - Click **Microsoft Office** button, and choose **Prepare**, and then click **View Signatures**. The **Signatures** (see figure on page 97) pane will be displayed.

     In the **Signatures** pane, right-click the signature name or the signature line, and then click **Signature Setup**.
   - In MS Office 2010, right-click the signature line, and then click **Signature Setup**.
2. In the **Signature Setup** (see figure on page 101) window, make the necessary changes and click **OK**.

Note: After you sign a signature line, you may view its properties in the **Signature Setup** window, but you can't edit it after signing.

Adding a Signature Line to a Document

In Microsoft Word 2007 and Word 2010, Excel 2007 and Excel 2010 programs, you can sign a signature line.

Note: If you will open a Microsoft Office 2007 document in previous versions of MS office, the signature line will be replaced by the common image and you can't sign it.

To add a signature in a signature line:

1. Depending on the MS Office software version, do one of the following:

   - In MS Office 2007, click **Microsoft Office** button, and choose **Prepare**, and then click **View Signatures**. The **Signatures** (see figure on page 97) pane will be displayed.

     In the **Signatures** pane, right-click the signature name or the signature line, and then click **Signature Setup**.

   - In MS Office 2010 right-click a signature string, and choose **Sign**.

2. In the **Sign** window, type your name or click **Select Image** link, if you want to paste a graphical image of a signature line. Below is a brief description of the certificate, which the document will sign. To sign a document, using another certificate, click **Change** and choose another certificate.

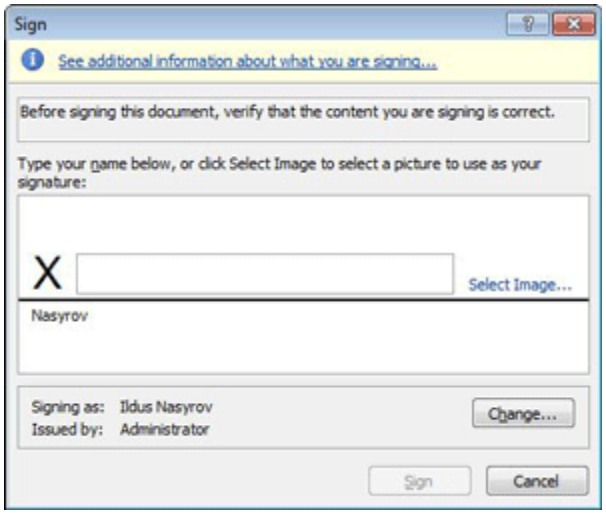
Sign
See additional information about what you are signing...
Before signing this document, verify that the content you are signing is correct.
Type your name below, or click Select Image to select a picture to use as your signature:
X
Select Image...
Nasyrov
Signing as: Ildus Nasyrov
Issued by: Administrator
Change...
Sign
Cancel

Figure 49: Signing a signature line

3. After you type a name and choose a certificate, click **Sign**. The **ViPNet CSP — Key Container Password** (see figure on page 79) window will be displayed.

4. Type your password and click **OK**. In the signature line the signer's name or signature graphical image will be displayed.

   If by some reasons the program can't verify the authenticity of certificate, the mark **Invalid Signature** will be displayed above the signature line.

Figure 50: An invalid signature

Note: You can sign an Invalid signature line again. To do it, right-click on the signature line (or on the signature name on the **Signatures** panel) and choose **Sign again**.

To view signature details (see Viewing a Digital Signature on page 96) or to remove signature (see Removing a Digital Signature on page 99) from visible signature line is the same as in the case of the invisible signature:

1. Depending on the MS Office software version, do one of the following:
   - In MS Office 2007, click **Microsoft Office** button, point to **Prepare**, and then click **View Signatures** (or click the digital signature icon on the status bar of the document).
   - In MS Office 2010, click the **File** tab, and then click **View signatures**.

   The **Signatures** (see figure on page 97) pane will be displayed.
2. In the **Signatures** pane, right-click the signature name or the signature line. Depending of what you need to do, click **Signature Details** or **Remove signature**.

Digital Signature and Encryption in Microsoft Mail Programs

Organizing Encrypted Messages Exchange	106
Exchanging Certificates with the Message Recipient	107
Advanced Configuring of Digital Signature and Encryption	109
Adding a Digital Signature to All Messages	111
Adding a Digital Signature to a Message	116
Viewing the Message's Digital Signature	119
Email Encryption	121
Viewing the Encrypted Messages	126
Encrypting Documents and Files	127

Organizing Encrypted Messages Exchange

This section describes encrypted messages exchange between ViPNet CSP and Microsoft Outlook mail programs (2003, 2007 or 2010 versions) and Microsoft Windows Live (2009 version). To organize encrypted messages exchange between ViPNet CSP and one of these mail programs:

1. Install (see Ways to Install a Private Key and a Certificate on page 60) the container and the certificate in ViPNet CSP, and install the issuer's certificate and CRL (see Installing Issuer's Certificates and CRL on page 73).
2. Exchange certificates with the recipient (sender) of the message (see Exchanging Certificates with the Message Recipient on page 107).
3. If necessary, you can configure a mail program for working with a digital signature and encrypted (see Advanced Configuring of Digital Signature and Encryption on page 109). messages.
4. Depending on whether you are a sender or a recipient of an encrypted message:
   - Sign a message using your digital signature (see Adding a Digital Signature to All Messages on page 111, Adding a Digital Signature to a Message on page 116).
   - Create and send an encrypted message (see Email Encryption on page 121).
   - Decrypt the received message (see Viewing the Encrypted Messages on page 126).

Warning: To sign email messages, you need a public key certificate where the certificate owner's email address is specified and, in the Enhanced Key Usage box, the attribute Secure Email is enabled. If you don't have such a certificate, you can't add a digital signature to a message.

To sign email messages, create a request for a new certificate, specify your email address and deliver your request to the administrator of your Certification authority.

Microsoft Outlook and Windows Live programs allow you not only exchange encrypt messages, but also encrypt documents and files (see Encrypting Documents and Files on page 127).

Exchanging Certificates with the Message Recipient

To encrypt an email message, you need a certificate of its recipient. You can exchange certificates by:

- Sending a message with a digital signature (see Adding a Digital Signature to a Message on page 116). Saving the sender's email into contacts, the recipient adds the sender's certificate.
- Sending the certificate file (`.cer`) to a recipient in an email message or a removable drive. Or storing the certificate file in a public network store. This feature allows the recipient to import the certificate file into contacts.
- Creating and sending a contact with the certificate file.

Warning: he recipient's certificate and your certificate should contain the owner's email addresses (see Email Address of the Certificate Is Not Found on the List of Contact Addresses on page 159).

To import the certificate into contacts:

1. In the Microsoft Outlook or Microsoft Windows Live program, in the navigation pane, choose **Contacts**.
2. Double-click the required contact.
3. Open the window for managing the user's certificates:
   - In the Outlook 2003 program, open the **Certificates** tab.
   - In the Outlook 2007 or Outlook 2010 program, on the **Contact** tab, under **Show**, click **Certificates** .
   - In the Windows Live Mail program, choose the **IDs** section.
4. Click **Import**.
5. In the **Select digital ID file to import** window, specify the path to the certificate file, and click **Open**.

   The chosen certificate will be added to this contact.

6 To make sure that you can trust the added certificate, choose it and click **Properties**.

   If, in the **Certificate** window, on the **General** tab, the or is displayed, the certificate can't be trusted.

7 If the certificate is not trusted, in the **Certificate** window, on the **General** tab, click **Trust this certificate**. Then click **OK**.

Warning: If after the certificate's import a message is displayed that the email address specified in this certificate is not found in the list (see Email Address of the Certificate Is Not Found on the List of Contact Addresses on page 159) then you can't encrypt an email message using this certificate.

To send the contact's card with a certificate:

1 In the Microsoft Outlook or Windows Live Mail program, create a new contact and fill contact with your data.

2 Import your certificate into a contact.

3 On the contact context menu:

- In the Outlook 2003 program, click **Forward**.
- In the Outlook 2007 program, click **Send Full Contact**, and then choose **In Outlook Format**.
- In the Outlook 2010 program, click **Forward**, and then choose **As an Outlook Contact**.

4 In the message window, specify the recipient's address, add a text, and then click **Send**.

Note: You can't send a contact in the Windows Live Mail program.

After you have exchanged certificates with the recipient, you can start sending encrypted messages.

Advanced Configuring of Digital Signature and Encryption

In the Microsoft Outlook program, to choose a signing or encryption certificate, a cryptographic message format, or to make some other settings, do the following:

1. Open the **Change Security Settings** window:
   - In Microsoft Outlook 2003, on the **Tools** menu, select **Options**, go to the **Security** tab, and click **Settings**.
   - In Microsoft Outlook 2007, on the **Tools** menu, select **Trust Center**, and then select the **E-mail Security** section, and click **Settings**.
   - In Microsoft Outlook 2010 or in Microsoft Outlook 2013, on the **File** tab, click **Options**. In the **Outlook Options** window, select the **Trust Center** section, and click **Trust Center Settings**. In the **Trust Center** window, select **E-mail Security section**, and click **Settings**.
2. In the **Cryptography Format** list, choose **S/MIME**.
3. Click **Choose** near the **Signing Certificate** box and specify the certificate.

Figure 51: Choosing a certificate for signing and encrypting

4. Click **Choose** near the **Encryption Certificate** box and specify the certificate.

Warning: If the certificate chosen for creating a digital signature does not contain any email address or the specified email address does not correspond to the outgoing message's address, you can choose this certificate as a digital signature certificate.

If the chosen certificate does not contain an outgoing email address, the following problems may occur:

- In the system store, there is another certificate with the email address similar to the outgoing email address. When you sign your email message, the digital signature will be created using this certificate, but not using the certificate specified before.
- In the system store, there are no certificates with the email address similar to the outgoing email address. When you try to sign the message, the digital signature will not be added.

To sign an email message with a certificate, create a request for a new certificate, specify the correct email address, and send your request to your certification authority administrator.

5 If necessary, configure other options and click **OK**.

To choose a certificate in the Windows Live Mail program:

1 On the **Tools** menu, click **Accounts**.

2 In the **Accounts** window, choose an account and click **Properties**.

3 In the account properties window, click the **Security** tab.

4 Under **Signing certificate**, near the **Certificate** box, click Select and specify the necessary certificate, which you will use to sign messages.

5 Under **Encrypting preferences**, near the **Certificate** box, click Select and specify the necessary certificate, which you will use to sign messages.

6 In the **Algorithm** list, choose an encryption algorithm.

7 Click **OK**.

Adding a Digital Signature to All Messages

Microsoft mail clients allow you to add a digital signature to email messages, to guarantee the authenticity and integrity of your message, and also to ensure non-repudiation. To ensure the confidentiality of a message, you need to encrypt it (see Email Encryption on page 121).

Below you can find the scenario of adding a digital signature to your outgoing messages in the Microsoft Outlook and Windows Live Mail programs.

Warning: To sign email messages, you need a public key certificate where the certificate owner's email address is specified and, in the Enhanced Key Usage box, the attribute Secure Email is enabled. If you don't have such a certificate, you can't add a digital signature to a message.

To sign email messages, create a request for a new certificate, specify your email address and deliver your request to the administrator of your Certification authority.

Microsoft Outlook

To add a digital signature to all messages:

1. Open the email security management window. To do this:

   If you use Microsoft Outlook 2003:

   - On the **Tools** menu, select **Options**.
   - In the **Options** window, click the **Security** tab.

   If you use Microsoft Outlook 2007:

   - On the **Tools** menu, select **Trust Center**.
   - In the **Trust Center** window, click the **E-mail Security** tab.

   If you use Microsoft Outlook 2010 or 2013:

   - Click the **File** tab and select **Options**. In the **Outlook Options** window, select **Trust Center** and click **Trust Center Settings**.
   - In the **Trust Center** window, select the **E-mail Security** section.

2 Under **Encrypted e-mail**, select the **Add digital signature to outgoing messages** check box.

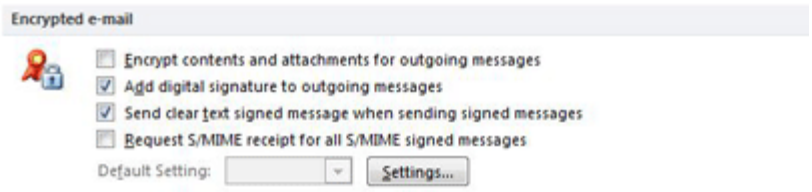
Encrypted e-mail
Encrypt contents and attachments for outgoing messages
Add digital signature to outgoing messages
Send clear text signed message when sending signed messages
Request S/MIME receipt for all S/MIME signed messages
Default Setting:
Settings...

Figure 52: Configuring encrypted e-mail parameters in the Trust Center window

3 Make sure that the **Send clear text signed message when sending signed messages** check box is selected (otherwise the recipients, who do not use the S/MIME protocol, can't read your message).

4 Click **Settings**. The **Change Security Settings** window will be displayed.

Figure 53: The Change Security Settings window

5 Fill the **Security Settings Name** box.

6 Click **Choose** near the **Signing Certificate** box.

7 In the **Select a Certificate** window, select a certificate from the list. To view a certificate, click the **Click here to view certificate properties** link.

After choosing the certificate, click **OK**. The same certificate will be automatically chosen for encryption.

Warning: If the certificate chosen for creating a digital signature does not contain any email address or the specified email address does not correspond to the outgoing message's address, you can choose this certificate as a digital signature certificate.

If the chosen certificate does not contain an outgoing email address, the following problems may occur:

- In the system store, there is another certificate with the email address similar to the outgoing email address. When you sign your email message, the digital signature will be created using this certificate, but not using the certificate specified before.
- In the system store, there are no certificates with the email address similar to the outgoing email address. When you try to sign the message, the digital signature will not be added.

To sign an email message with a certificate, create a request for a new certificate, specify the correct email address, and send your request to your certification authority administrator.

8 To save the settings, double-click **OK**.

Windows Live Mail

To add a digital signature to all messages:

1 In the main Windows Live Mail window, on the **Tools** menu, select **Safety Options**.

2 In the **Safety Options** window, click the **Security** tab.

3 Under **Secure Mail**, select the **Digitally sign all outgoing messages** check box.

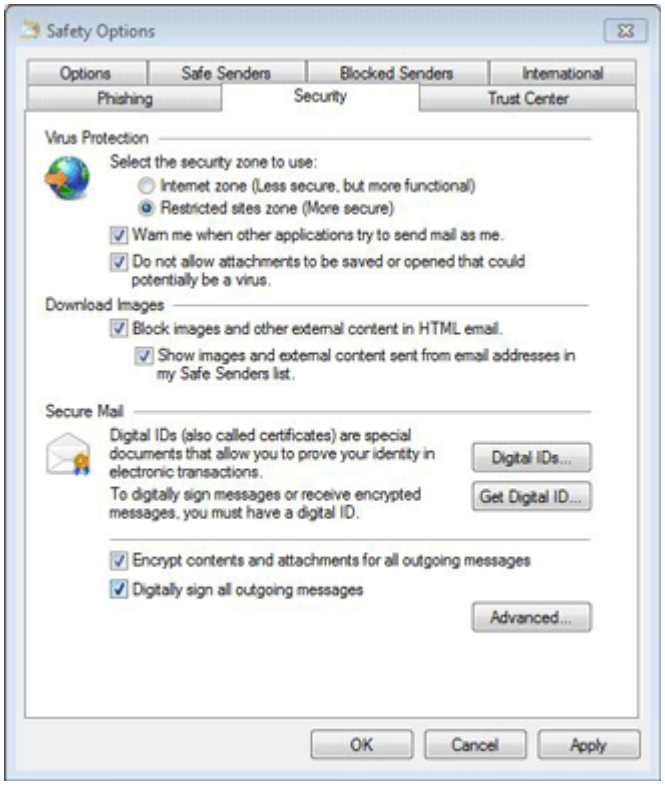
Safety Options
Options
Safe Senders
Blocked Senders
International
Phishing
Security
Trust Center
Virus Protection
Select the security zone to use:
Internet zone (Less secure, but more functional)
Restricted sites zone (More secure)
Warn me when other applications try to send mail as me.
Do not allow attachments to be saved or opened that could potentially be a virus.
Download Images
Block images and other external content in HTML email.
Show images and external content sent from email addresses in my Safe Senders list.
Secure Mail
Digital IDs (also called certificates) are special documents that allow you to prove your identity in electronic transactions.
Digital IDs...
To digitally sign messages or receive encrypted messages, you must have a digital ID.
Get Digital ID...
Encrypt contents and attachments for all outgoing messages
Digitally sign all outgoing messages
Advanced...
OK
Cancel
Apply

Figure 54: Adding a digital signature to all outgoing messages

4 Click **Advanced**. The **Advanced Security Settings** window will be displayed.

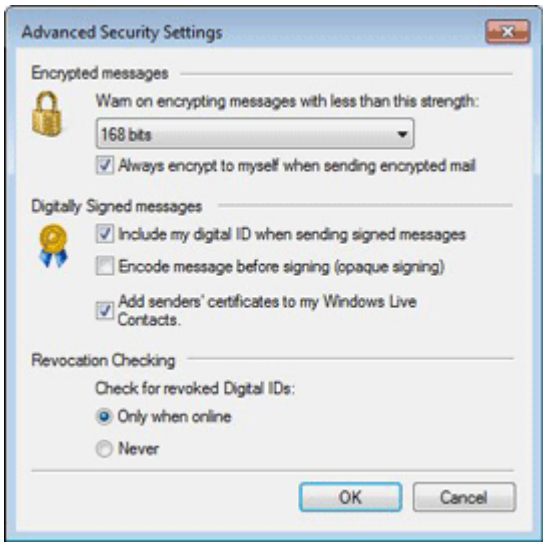
Advanced Security Settings
Encrypted messages
Warn on encrypting messages with less than this strength:
168 bits
Always encrypt to myself when sending encrypted mail
Digitally Signed messages
Include my digital ID when sending signed messages
Encode message before signing (opaque signing)
Add senders' certificates to my Windows Live Contacts.
Revocation Checking
Check for revoked Digital IDs:
Only when online
Never
OK
Cancel

Figure 55: Advanced security settings

5 Make sure that the **Include my digital ID when sending signed messages** check box is selected.

6 Make sure that the **Add senders' certificates to my Windows Live Contacts** check box is selected.

7 To save the settings, double-click **OK**.

Adding a Digital Signature to a Message

To add a digital signature to a single message, follow the instructions in this section.

Warning: To sign email messages, you need a public key certificate where the certificate owner's email address is specified and, in the Enhanced Key Usage box, the attribute Secure Email is enabled. If you don't have such a certificate, you can't add a digital signature to a message.

To sign email messages, create a request for a new certificate, specify your email address and deliver your request to the administrator of your Certification authority.

Microsoft Outlook

To digitally sign your message:

1. Create a new message and depending on the Microsoft Office software version do one of the following:
   - In Microsoft Outlook 2003, on the toolbar, click **Digitally Sign** .
   - In Microsoft Outlook 2007, click the **Message** tab. Under **Options**, click **Digitally Sign** .
   - In Microsoft Outlook 2010, click the **Options** tab. Under **Permission**, click **Sign** .
   - In Microsoft Outlook 2013, click the **Options** tab. Under **Permission**, click **Sign** .

   Note: The **Digitally Sign** or **Sign** ( ) buttons may be missing from the toolbar if you have not chosen the certificate set by default in the **Change Security Settings** (see Adding a Digital Signature to All Messages on page 111) window.

2. If there is no **Digitally Sign** (or **Sign** /) button, refer to Digitally Sign/Sign Button Isn't Displayed. (see Digitally Sign/Sign Button Isn't Displayed on page 117)
3. Type your message, and specify a subject and the recipient. If necessary, you may add an attachment.

4 Click **Send**. The **ViPNet CSP — Key Container Password** (see figure on page 79) window will be displayed.

5 Type your password and click **OK**.

Digitally Sign/Sign Button Isn't Displayed

In case the **Digitally sign**/**Sign** button is not displayed:

1 Open the **Security Properties** window. To do this, depending on the Microsoft Office software version, do one of the following:

- In Microsoft Outlook 2003, click **Options**, then, in the **Message Options** window, click **Security Settings**.
- In Microsoft Outlook 2007, click the **Options** tab, click **More Options**. In the **Message Options** window, click **Security Settings**.
- In Microsoft Outlook 2010 or Microsoft Outlook 2013, click the **Options** tab, and, under **More Options**, click **Properties** . In the **Properties** window, click **Security Settings**.

The **Security Properties** window will be displayed.

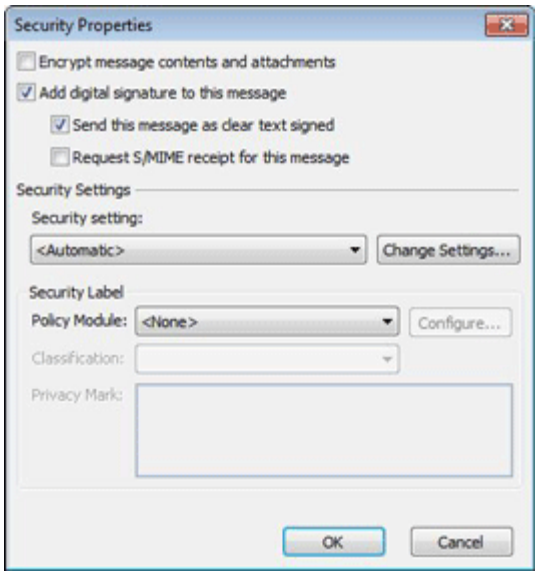

Figure 56: Security Properties window

2 Select the **Add digital signature to this message** check box.

3 If necessary, in the **Security setting** list, choose preset parameters of signing and encrypting.

By default in the **Security setting** list, the value is set to **<Automatic>**. This means that the certificate will be chosen automatically. To choose the certificate manually, click **Change Settings** (see Advanced Configuring of Digital Signature and Encryption on page 109).

4 To save the settings, click **OK**.

Windows Live Mail

To digitally sign a message:

1 Create a new message in the Windows Live Mail program.

2 In the **New message** window, on the **Tools** menu, select **Digitally sign**.

Note: If, in the **New message** window, the menu is not displayed, on the toolbar, click and select **Show menu bar**.

---

3 Type your message, specify the subject and the recipient. If necessary, you may add an attachment.

4 Click **Send**. The **ViPNet CSP — Key Container Password** (see figure on page 79) window will be displayed.

5 Type your password and click **OK**.

Viewing the Message's Digital Signature

Microsoft Outlook

To verify a message's digital signature, do the following:

1. Open the message with a digital signature.
2. In the **Signed by** status line, check the email address of the user who signed the message.

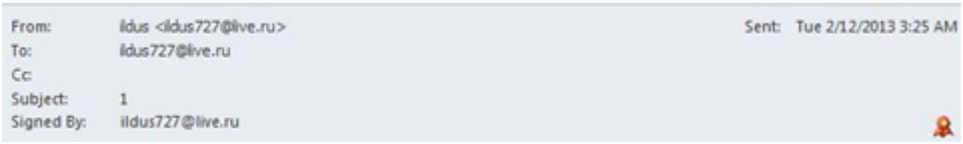

Figure 57: Verifying the digital signature of the message

> **Warning:** If the email address in the **Signed by** status line does not match the senders' address, specified in the **From** line, then the true sender is the user who signed this message.

If during the digital signature verification some problems occur, the **Signed by** status line will be underlined.

Figure 58: Message with an invalid digital signature

3. To see more information about this problem, click **Digital Signature** . The **Digital Signature: Valid** window will be displayed. If a digital signature you want to use is not valid, the **Digital Signature: Invalid** window will be displayed.
4. For more information about the certificate, click **Details**.

Windows Live Mail

To verify a message's digital signature, do the following:

1. Choose the signed message from the list.
2. In the reading pane, in the message header, the icon of a digital signature will be displayed.

   If during the digital signature verifying some problems occurs, you will be warned informed that you can't trust this digital signature (this information will be displayed in the message header with the red background). Message text will be replaced with Security Warning.

   If the message is signed with an invalid digital signature, you can do the following:

   - To view the message, click **Open message**.
   - To view the certificate the message has been signed with, click **View Certificate**.
   - To add the certificate which the messages was signed with to trusted certificates, click **Change the rules of trust**.

Email Encryption

Email Encryption in Outlook 2003

To encrypt a message:

1. In the Outlook program, create a new message and specify the recipient.
2. In the email message window, do one of the following:
   - On the toolbar, click **Encrypt**.
   - Click **Options**. Then in the **Message Options** window, click **Security Settings** and select the **Encrypt message contents and attachments** check box.

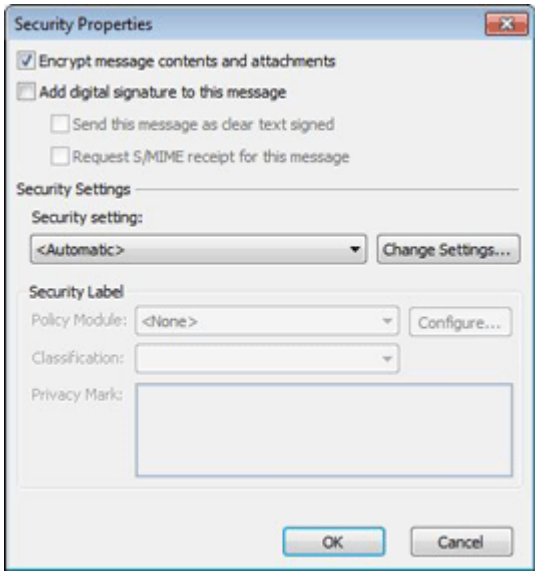

Figure 59: Configuring parameters for encrypting a message

3. To change additional settings (see Advanced Configuring of Digital Signature and Encryption on page 109), such as using a specific certificate, click **Change Settings**.
4. Click **OK** three times.
5. Send the encrypted message to the recipient.

Tip: If during sending an encrypted message an error message is displayed, see Problems and Troubleshooting (on page 150).

To encrypt all outgoing messages:

1. In the main Outlook window, on the **Tools** menu, click **Options**, and then click the **Security tab**.
2. Select the **Encrypt contents and attachments for outgoing messages** check box.

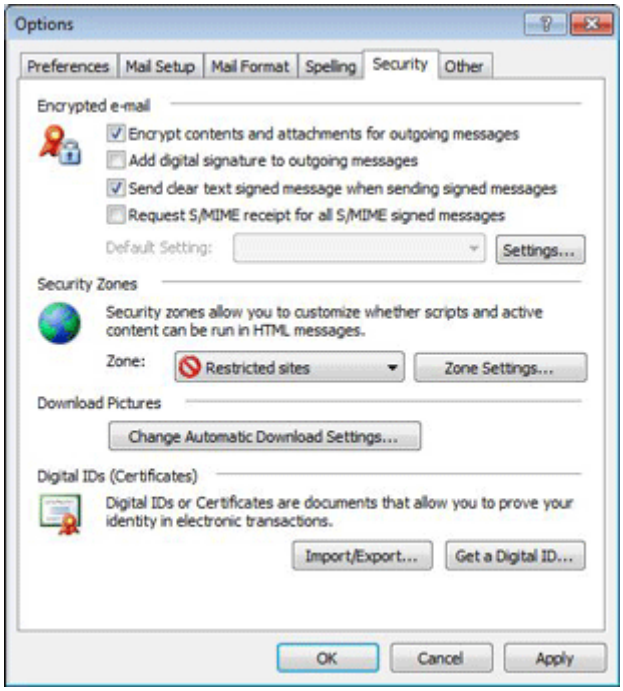

Figure 60: Configuring all messages encryption

3. To choose your certificate for signing and encrypting, click **Settings** and, in the **Change Security Settings** window, select the required certificates.
4. After that, all your outgoing messages will be encrypted if the certificate has been added to the recipient's contact card.

Email Encryption in Outlook 2007

To encrypt a single email message:

1. Create a new message in the Outlook program and specify the recipient.
2. Enable encryption in one of the following ways:
   - In the message, on the **Message** tab, under **Options**, click **Encrypt**.

- In the message, on the **Message** tab, under **Options**, open the **Security Settings** (see figure on page 121), and select **Encrypt message contents and attachments** check box.

  To change additional settings (see Advanced Configuring of Digital Signature and Encryption on page 109), such as using a specific certificate, click **Change Settings**.

3. Send your message.

To encrypt all outgoing messages:

1. In the main Outlook window, on the **Tools** menu, click **Trust Center**, and then click **E-mail Security**.
2. Under **Encrypted e-mail**, select the **Encrypt contents and attachments for outgoing messages** check box.
3. To change additional settings (see Advanced Configuring of Digital Signature and Encryption on page 109), such as choosing a specific certificate, click **Settings**.
4. Double-click **OK**.
5. After that, all your outgoing messages will be encrypted if the recipient's certificates have been added to the contacts.

Email Encryption in Microsoft Outlook 2010 and Microsoft Outlook 2013

To encrypt a single email message:

1. Create a new message in the Outlook program and specify the recipient.
2. Enable the encryption function using one of the following:
   - In the message, on the **Options** tab, under **Permission**, click **Encrypt** (**Encrypt**).
   - In the message, open the **Options** tab, and under **More Options**, click **Properties** . In the **Properties** window, click **Security Settings**.

     In the **Security Properties** (see figure on page 121) window, select the **Encrypt message contents and attachments** check box.

     To change additional settings (see Advanced Configuring of Digital Signature and Encryption on page 109), such as choosing a specific certificate, click **Change Settings**.

3 Send a message.

To encrypt all outgoing messages:

1 In the main Outlook window, on the **File** tab, click **Options**.

2 In the **Outlook Options** window, select **Trust Center**, and click **Trust Center Settings**.

3 In the **Trust Center** window, select the **E-mail Security** section. Under **Encrypted e-mail**, select the **Encrypt contents and attachments for outgoing messages** check box.

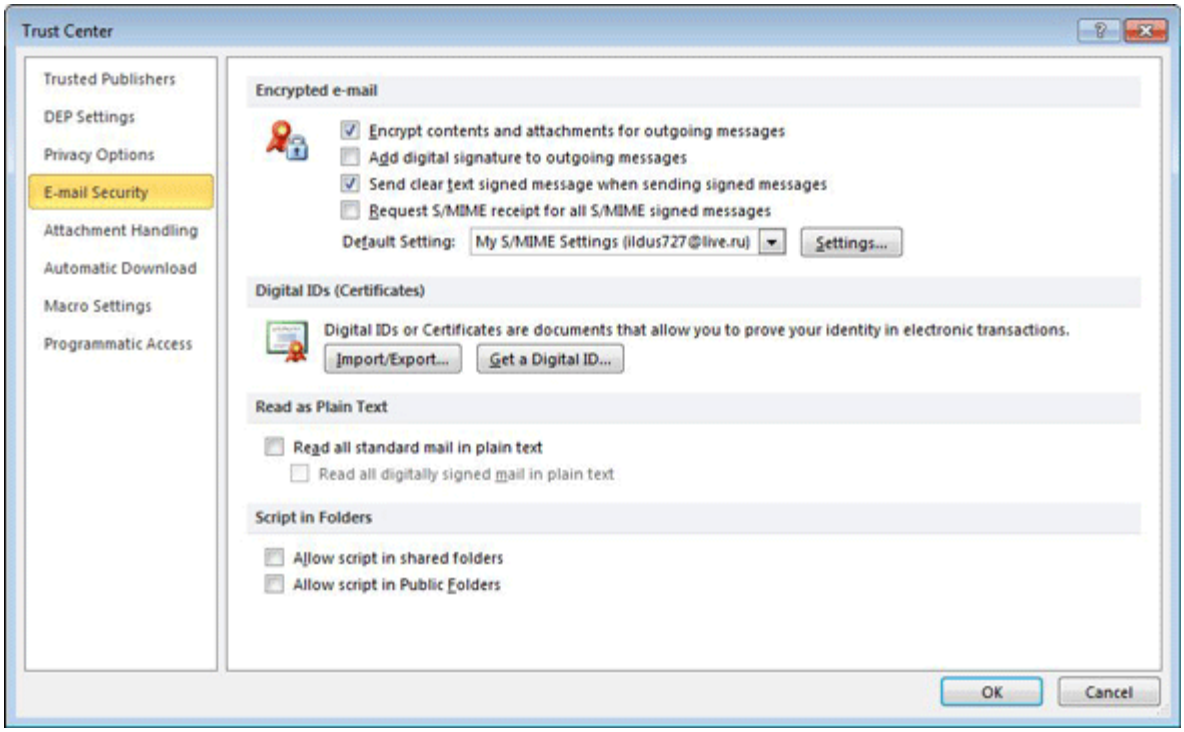
Trust Center
Trusted Publishers
DEP Settings
Privacy Options
E-mail Security
Attachment Handling
Automatic Download
Macro Settings
Programmatic Access
Encrypted e-mail
Encrypt contents and attachments for outgoing messages
Add digital signature to outgoing messages
Send clear text signed message when sending signed messages
Request S/MIME receipt for all S/MIME signed messages
Default Setting:
My S/MIME Settings (ildus727@live.ru)
Settings...
Digital IDs (Certificates)
Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.
Import/Export...
Get a Digital ID...
Read as Plain Text
Read all standard mail in plain text
Read all digitally signed mail in plain text
Script in Folders
Allow script in shared folders
Allow script in Public Folders
OK
Cancel

Figure 61: Configuring parameter for encrypting all messages

4 To change additional settings (see Advanced Configuring of Digital Signature and Encryption on page 109), such as choosing a specific certificate, click **Settings**.

5 Double-click **OK**.

6 After that, all your outgoing messages will be encrypted if the recipient's certificates have been added to the contacts.

Email Encryption in the Windows Live Mail Program

To encrypt an email message:

1. Create a new message in Windows Live Mail and specify the recipient.
2. In the **New message** window, on the **Tools** menu, select **Encrypt**.

> **Note:** If, in the **New message** window, the menu is not displayed, click on the toolbar and select the **Show** menu bar.

3. Send a message.

To encrypt all outgoing messages:

1. In the main Windows Live Mail window, on the **Tools** menu, select **Safety Options**.
2. In the **Safety Options** window, click the **Security** (see figure on page 114) tab.
3. Under **Secure Mail**, select the **Encrypt contents and attachments for all outgoing messages** check box.
4. Click **OK**.

   After that, all your outgoing messages will be encrypted if the recipient's certificates were added to the contacts.

Viewing the Encrypted Messages

The encrypted message you've received is marked with (in Microsoft Outlook) or (in Microsoft Windows Live).

When you choose an encrypted message in the Microsoft Outlook program, in the reading pane, the notification message will be displayed: "This item can't be displayed in the Reading Pane. Open the item to read its contents." In the Windows Live Mail program, when you choose an encrypted message, you are prompted to type the password to the key container. Thus, your message is protected from unauthorized access.

Warning: You need the ViPNet CSP program to view an encrypted message.

To view an encrypted message:

1. In the Microsoft Outlook program, double-click the required message in the list. In the Windows Live Mail program, choose the required message from the list. In Windows Live Mail, choose a message from a list.
2. In the **ViPNet CSP — Key Container Password** (see figure on page 79) window, type the password used for your private key protection.

   After that the message with all its attachments will be decrypted and displayed in the reading pane.

Encrypting Documents and Files

If you want to encrypt certain documents or files, you can do one of the following:

1. Create an encrypted message (see Email Encryption on page 121).
2. Specify necessary documents or files as an attachment.
3. Send a message to the recipient or to yourself. In the first case, only specified recipient can view encrypted documents, in the second one, only you.

11

Digital Signature in Microsoft Office InfoPath

Permission to Sign an InfoPath Form with a Digital Signature	129
Signing an InfoPath Form	133
Viewing an InfoPath Form Signature	136
Unsigning an InfoPath Form	137

Permission to Sign an InfoPath Form with a Digital Signature

When you are creating a form template in Microsoft Office InfoPath, you may allow users to digitally sign it. Filling in the form, users can sign the whole form or its parts.

Microsoft Office InfoPath 2003

To allow users to sign a Microsoft Office InfoPath 2003 form, do the following:

1. Create or open a form template in the constructor mode.
2. On the **Tools** menu, click **Form Options**.
3. In the **Form Options** window, on the **Digital Signatures** tab, select the **Enable digital signatures for the entire form** check box.
4. If necessary, select the **Prompt user to sign the form if it is submitted without a signature** check box.
5. To save the settings, click **OK**.

Microsoft Office InfoPath 2007

To allow users to sign a Microsoft Office InfoPath 2007 form, do the following:

1. Create or open a form template in a constructor mode.
2. On the **Tools** menu, click **Form Options**.
3. In the **Form Options** window, click the **Digital Signatures** tab.

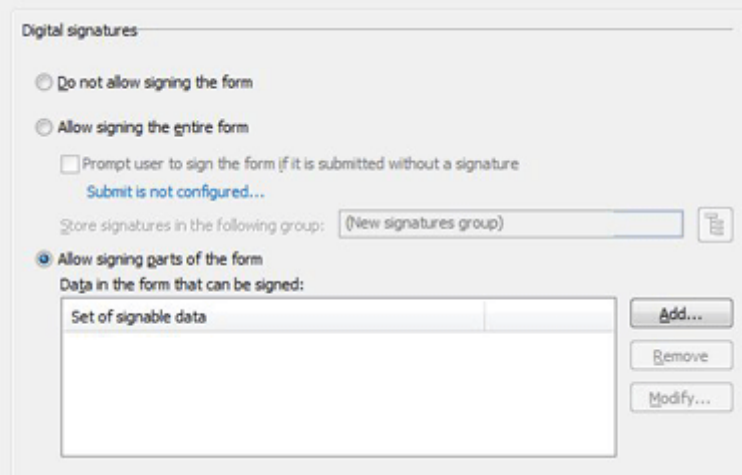
Digital signatures
Do not allow signing the form
Allow signing the entire form
Prompt user to sign the form if it is submitted without a signature
Submit is not configured...
Store signatures in the following group:
(New signatures group)
Allow signing parts of the form
Data in the form that can be signed:
Set of signable data
Add...
Remove
Modify...

Figure 62: The Digital Signatures tab

4 If you want the user to sign the entire form, choose the **Enable digital signatures for the entire form**.

If necessary, you may also select the **Prompt user to sign the form if it is submitted without a signature** check box.

5 If you want the user to sign a part of the form, choose the **Enable digital signatures for specific data in the form**.

- To specify data for signing, click **Add**. The **Set of Signable Data** window will be displayed.

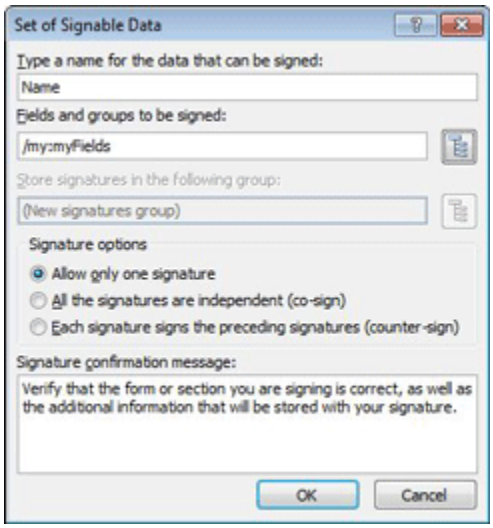
Set of Signable Data
Type a name for the data that can be signed:
Name
Fields and groups to be signed:
/my:myFields
Store signatures in the following group:
(New signatures group)
Signature options
Allow only one signature
All the signatures are independent (co-sign)
Each signature signs the preceding signatures (counter-sign)
Signature confirmation message:
Verify that the form or section you are signing is correct, as well as the additional information that will be stored with your signature.
OK
Cancel

Figure 63: The Set of Signable Data window

- Type the name of the data intended for signing in the corresponding box.

- Click **Select XPath** next to the **Fields and Groups to be signed** box.
- In the **Select a Field or Group** window, choose the field which you want to sign and click **OK**.
- To specify the relation type between several signatures, select the required type (the **Allow only one signature** is specified by default), and add a message to confirm the signature.
- To save the settings, click **OK**. The chosen field will be displayed in the **Set of Signable Data** (see figure on page 130) list.
- If you want the user to sign several form fields, repeat the step 5 as many times as necessary.

6 To save the settings, click **OK**.

Microsoft Office InfoPath 2010

To allow users to sign a Microsoft Office InfoPath 2010 form, do the following:

1 Create or open a form template in the constructor mode.

2 Click the **File** tab and, in the **Info** section, click **Form Options**.

3 In the **Form Options** window, click the **Digital Signatures** tab.

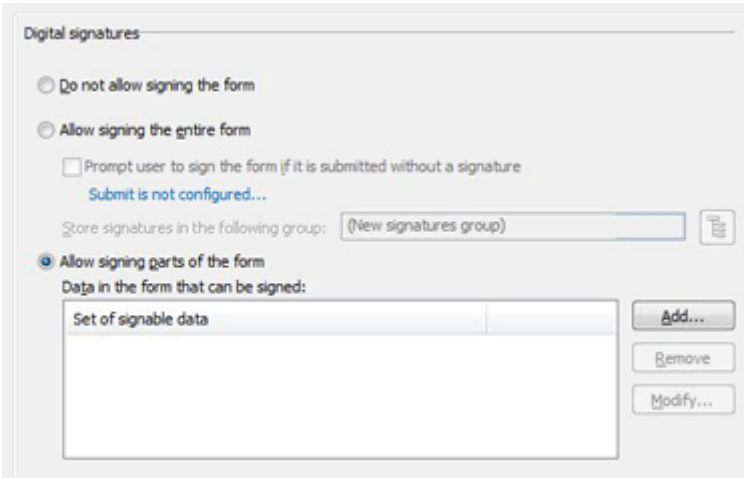
Digital signatures
Do not allow signing the form
Allow signing the entire form
Prompt user to sign the form if it is submitted without a signature
Submit is not configured...
Store signatures in the following group:
(New signatures group)
Allow signing parts of the form
Data in the form that can be signed:
Set of signable data
Add...
Remove
Modify...

Figure 64: The Digital Signatures tab

4 To specify data for signing, click **Add**.

5 The **Set of Signable Data** window will be displayed.

- Type the name of the data intended for signing in the corresponding box.

- Click **Select XPath** next to the **Fields and Groups to be signed** box.
- In the **Select a Field or Group** window, choose the field which you want to sign and click **OK**.
- To specify the relation type between several signatures, select the required type (the **Allow only one signature** is specified by default), and add a message to confirm the signature.
- To save the settings, click **OK**. The chosen field will be displayed in the **Set of Signable Data** (see figure on page 130) list.

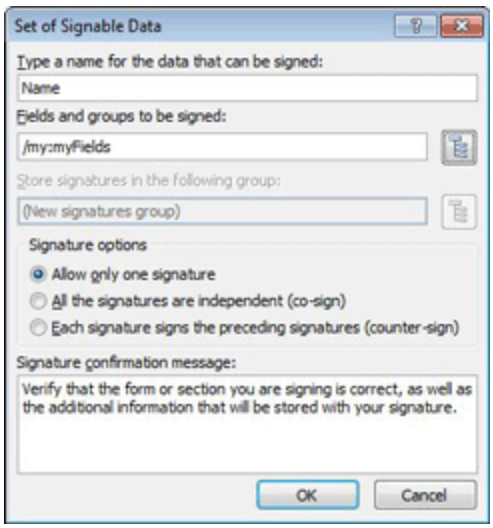
Set of Signable Data
Type a name for the data that can be signed:
Name
Fields and groups to be signed:
/my:myFields
Store signatures in the following group:
(New signatures group)
Signature options
Allow only one signature
All the signatures are independent (co-sign)
Each signature signs the preceding signatures (counter-sign)
Signature confirmation message:
Verify that the form or section you are signing is correct, as well as the additional information that will be stored with your signature.
OK
Cancel

Figure 65: The Set of Signable Data window

6 To save the settings, click **OK**.

Signing an InfoPath Form

When creating a form, you can allow a user to digitally sign this form. Information of how a user can sign the form is given below.

Microsoft Office InfoPath 2003

To sign a form, do the following:

1. Open a form or a template.
2. On the **Tools** menu, select **Digital signatures** (or, on the toolbar, click **Digital Signatures**). The **Digital Signatures** window will be displayed.

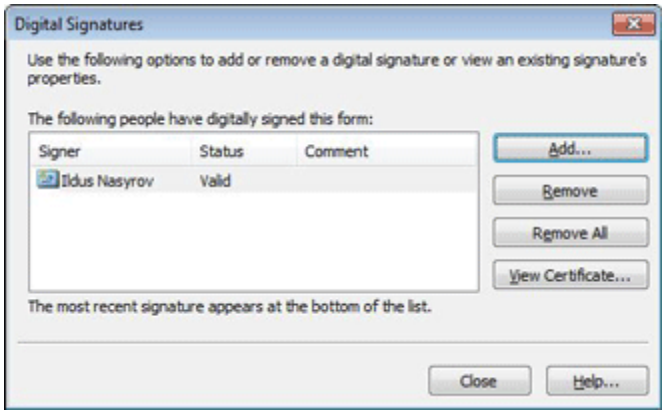

Figure 66: The Digital Signatures window

3. Click **Add** and, in the **Digital Signature Wizard** window, click **Select Certificate**.
4. Select your certificate from the list. To open the certificate, click **View Certificate**. After choosing the certificate, click **OK**.
5. In the **Comment** box, type a comment, which will be included in your signature. Click **OK**.
6. In the **ViPNet CSP — Key Container Password** (see figure on page 79) window, type the password and click **OK**.

You can't change the form after signing.

Microsoft Office InfoPath 2007, 2010, and 2013

To sign a form, do the following:

1. Open a form or a template in the InfoPath 2007, InfoPath Filler 2010, or InfoPath Filler 2013 program.
2. Depending on the Microsoft Office InfoPath software version, do one of the following:
   - In InfoPath 2007, on the **Tools** menu, select **Digital signatures** (or, on the toolbar, click **Digital Signatures**).
   - In InfoPath 2010, open the **File** tab and, in the **Info** section, click **Digital Signatures**.

   The **Digital Signatures** window will be displayed.

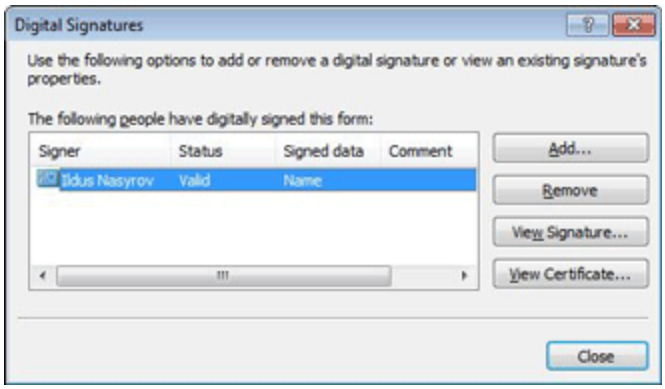

Figure 67: The Digital Signatures window

3. Click **Add**. The **Select the data to Sign** window will be displayed.
4. If a digital signature should be applied to the entire form, choose **Entire form**. If a digital signature should be applied to a part of the form, select the data you want to sign from the list.
5. Click **OK**. The **Sign** (see figure on page 103) window will be displayed.
6. If you are signing a separate data, type your name in the box next to the X, and click the **Select Image** link, to paste an image of your signature.
7. If necessary, fill in the **Purpose for signing this document** box. In InfoPath Filler 2013, this window also allows you to choose a signing reason from several pre-defined options in the **Commitment type** list.
8. In the **Sign** window, you can find a brief description of the certificate, which you use for signing the data. To sign a document using another certificate, click **Change**, and choose another certificate.

9 Click **Sign**. The **ViPNet CSP — Key Container Password** (see figure on page 79) window will be displayed.

10 Type your password and click **OK**.

You can't change the form or fields after signing.

Viewing an InfoPath Form Signature

To view a digital signature in a Microsoft InfoPath 2003 form:

1. Depending on the Microsoft InfoPath software version, do one of the following:
   - In Microsoft InfoPath 2003 or Microsoft InfoPath 2007, on the **Tools** menu, select **Digital signatures** (or, on the toolbar, click **Digital Signatures**).
   - In Microsoft InfoPath Filler 2010, click the **File** tab and, in the **Info** section, click **Digital Signatures**.
   - In Microsoft InfoPath Filler 2013, click the **File** tab and, in the **Info** section, click **View signatures**.

   The **Digital Signatures** window will be displayed.
2. If you use Microsoft InfoPath 2003, choose a certificate from the list and click **View Certificate**.

   If the certificate is untrusted, then, in the **Certificate** window, on the **General** (see figure on page 96) tab, a message informing you about the problem will be displayed. An untrusted certificate is marked with a red X.
3. In Microsoft InfoPath 2007, Microsoft InfoPath Filler 2010, or Microsoft InfoPath Filler 2013, choose a digital signature from the list and click **View Signature**. The **Signature Details** (see figure on page 98) window will be displayed.
   - The **Signature Details** window contains brief information about the signature and the certificate. If any certificate validation errors occur, the corresponding message will be displayed under the window title.
   - To open a certificate, click **View**. To view the additional signing information, click the **See the additional signing information that was collected** link.

Unsigning an InfoPath Form

To unsign a Microsoft InfoPath form:

1. Depending on the Microsoft InfoPath software version, do one of the following:
   - In Microsoft InfoPath 2003 or Microsoft InfoPath 2007, on the **Tools** menu, select **Digital signatures** (or, on the toolbar, click **Digital Signatures**).
   - In Microsoft InfoPath Filler 2010 or Microsoft InfoPath Filler 2013, click the **File** tab and, in the **Info** section, click **Digital Signatures**.

   The **Digital Signatures** window will be displayed.
2. Choose a digital signature from the list. To view a digital signature before unsigning:
   - In Microsoft InfoPath 2003 or Microsoft InfoPath Filler 2013, click **View Certificate**. The **Certificate** window will be displayed.
   - In Microsoft InfoPath 2007 or Microsoft InfoPath Filler 2010, click **View Signed Form**. The **Signature Details** window will be displayed. To open the certificate, click **View**.
3. After choosing a digital signature, click **Remove**.

Note: To remove all digital signatures at once, in Microsoft Office InfoPath 2003, click **Remove all**.

4. In the confirmation window, click **Yes**. The digital signature will be removed from the form.

12

Digital Signature for Macros and Databases

Macro Digital Signature	139
Signing Microsoft Access 2007 and 2010 Databases	142

Macro Digital Signature

Digitally Signing a Macro

In the Microsoft Office software, you can digitally sign a macro. Digital signature allows to confirm the origin of the macro and its security. You can create and sign a macro in Microsoft Word, Excel, Outlook, PowerPoint, Access, Publisher, and Visio.

Warning: For you to sign a macro, your certificate must contain a "Code signing" attribute of the Enhanced Key Usage field. If you don't have such a certificate, you can't sign a macro. To get a certificate with this attribute, contact your Key and Certification Authority administrator (see "ViPNet Administrator Key and Certification Authority. Administrator's Guide").

To sign a macro, do the following:

1. Open the Microsoft Visual Basic editor.
   - If you use Microsoft Office 2003 or Microsoft Outlook 2007, Publisher 2007, Visio 2007, on the **Tools** menu, select **Macro**, and the click **Visual Basic Editor**.
   - If you use Microsoft Word 2007, Excel 2007 or PowerPoint 2007, on the **Developer** tab, under **Code**, click **Visual Basic**.

     Note: By default, the **Developer** tab is not displayed. To display it, on the **File** menu, select **Options** and, in the opened window, in the Advanced section, select the **Developer** check box.

   - If you use Microsoft Access 2007, Microsoft Access 2010, or Microsoft Access 2013, on the **Database Tools** tab, under **Macro**, click **Visual Basic**.
   - If you use Microsoft Office 2010 or Microsoft Office 2013, except for Microsoft Access, on the **Developer** tab, under **Code**, click **Visual Basic**.

Note: To open Microsoft Visual Basic Editor in any of these applications, press **Alt+F11**.

2 In Microsoft Visual Basic editor, on the **Tools** menu, select **Digital Signature**. The **Digital Signature** window will be displayed.

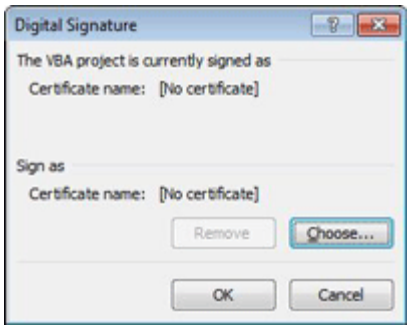

Figure 68: Adding a digital signature

3 Click **Choose**, choose a certificate from the list, and click **OK**. A digital signature will be added to a macro.

Verifying a Macro's Digital Signature

To verify a digital signature in a macro project, do the following:

1 In Microsoft Visual Basic editor, on the **Tools** menu, select **Digital Signature**. The **Digital Signature** window will be displayed.

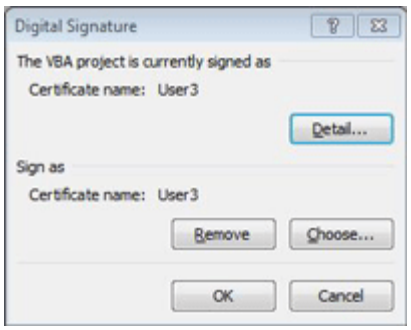

Figure 69: The Digital Signature window

2 In the **Digital signature** window, the current certificate is specified. To open certificate, click **Detail**.

If the chosen certificate is not valid, then, in the **Certificate** window, on the **General** (see figure on page 96) tab, the corresponding message will be displayed. The untrusted certificate is marked with a red X.

Unsigning a Macro

To remove a digital signature from a macro project, do the following:

1. In Microsoft Visual Basic editor, on the **Tools** menu, select **Digital Signature**. The **Digital Signature** (see figure on page 140) window will be displayed.
2. To remove a digital signature, click **Remove**. A digital signature will be removed from the project.

Signing Microsoft Access 2007 and 2010 Databases

Microsoft Access 2007 and Microsoft Access 2010 software allows you to sign databases during publishing. After you create a Microsoft Access 2007 or Microsoft Access 2010 database file, you can pack it and add a digital signature, and then share the signed package with other users. The users who received the package may extract the database from it and work with this database.

Note: You can't sign separate database components, if they were created in Microsoft Access versions earlier than Microsoft Access 2007. For more details, see Macro Digital Signature (on page 139).

To pack and sign a Microsoft Access database:

1. Depending on your software version, do one of the following:
   - In MS Office 2007, click **Microsoft Office** button, point to **Publish**, and then click **Package and Sign**.
   - In Microsoft Access 2010 program, on the **File** tab, click **Save & Publish**. Under **Save Database As**, click **Package & Sign**, and then click **Save As**.

   The **Select a Certificate** window will be displayed.
2. Choose a certificate and click **OK**. The **Create Microsoft Office Access Signed Package** window will be displayed.

   Warning: You can sign a database only using a certificate with the "Code signing" attribute of the Extended Key Usage extension. If you have no such attribute in your certificate, you can't create a signed package. To get a certificate with this attribute, contact your Key and Certification Authority administrator (see "ViPNet Administrator Key and Certification Authority. Administrator's Guide").
3. Choose a folder for saving signed package.
4. Type the name for the signed package in the **File name** box, and then click **Create**.

The signed package will be placed it in the folder that you have chosen.

13

Organizing a Protected Connection via TLS/SSL

Checklist: Organizing Access to a Protected Web Server 145

Configuring a Server Host 146

Configuring a Client Host 147

Configuring Internet Explorer for Work over the TLS/SSL Protocol 148

Checking the Web Host's Availability over the Secure HTTPS Protocol 149

Checklist: Organizing Access to a Protected Web Server

To organize access to a protected web server using the ViPNet CSP cryptographic service provider, you need to configure a server host and a web client host.

1. To configure a server host:
   - Configure IIS.
   - Install the ViPNet CSP cryptographic service provider.
   - In the system store, install the server's user certificate, the issuer's certificate (root certificate), and the actual CRL.

   For more information, see Configuring a Server Host (on page 146) section.
2. To configure a client host:
   - Install the ViPNet CSP cryptographic service provider.
   - In the system store, install the client's user certificate, the issuer's certificate (root certificate), and the actual CRL.
   - If necessary, configure Internet Explorer for work over the TLS/SSL protocol.

   For more information, see Configuring a Client Host (on page 147) section.

Configuring a Server Host

To configure the server host, do the following:

1. Configure IIS.
2. Install the ViPNet CSP cryptographic service provider (see Setting Up and Starting ViPNet CSP on page 25).
3. Create a certificate request for a server (see Creating a Certificate Request and Generating a Private Key on page 53) and send it to the Certification Authority.
4. Get a certificate for IIS, issued by request, from the administrator of your Certification Authority, and also get a root certificate and CRL.

Warning: Server user certificate should contain “Data Encipherment” attribute in the Key Usage field and “Client Authentication” attribute in the Enhanced Key Usage field.

5. Install the received certificate in a key container (see Installing Certificates in a Container on page 66).
6. In the system store of a local computer, install the server certificate (see Installing the User Certificate in the System Store on page 68), the issuer's certificate and the CRL (see Installing Issuer's Certificates and CRL on page 73).
7. Check that the network host is accessible over the secure HTTPS protocol (see Checking the Web Host's Availability over the Secure HTTPS Protocol on page 149).

Configuring a Client Host

To configure a client host, do the following:

1. Install the ViPNet CSP cryptographic service provider (see Setting Up and Starting ViPNet CSP on page 25).
2. Create a user certificate request for a web client (see Creating a Certificate Request and Generating a Private Key on page 53) and send it to the Certification Authority.
3. Get the certificate for a web client issued on your request and the issuer's certificate with a CRL from the administrator of your Certification authority.

Warning: The user certificate for a client host should contain “Client Authentication” attribute in Enhanced Key Usage field.

4. Install the received certificate in a key container (see Installing Certificates in a Container on page 66).
5. In the system store of the current user, install the received certificate (see Installing the User Certificate in the System Store on page 68), the issuer's certificate and the CRL (see Installing Issuer's Certificates and CRL on page 73).
6. Configure Internet Explorer for work over the secure protocol.
7. Check that the network host is accessible over the secure HTTPS protocol (see Checking the Web Host's Availability over the Secure HTTPS Protocol on page 149).

Configuring Internet Explorer for Work over the TLS/SSL Protocol

As a rule, default browser settings allow you to work over the TLS/SSL protocol. If the default settings have been changed or you can't connect to the server, do the following:

1. In the **Internet Options** window (**Tools: Internet Options**). To do this:
   - In the Internet Explorer **Tools** menu, click **Internet Options**.
   - In the Google Chrome and Yandex.Browser option windows, click **Change Proxy Settings**.
2. Click the **Details** tab.
3. Select the **SSL 3.0**, and **TLS 1.0** check boxes.
4. Clear the **SSL 2.0** check box.
5. Check that the network host is accessible over the secure HTTPS protocol (see Checking the Web Host's Availability over the Secure HTTPS Protocol on page 149).

Note: To work in Yandex.Browser and Google Chrome over the TLS/SSL protocol, in the shortcut properties, in the **Object** box, at the end of the path to the program folder add the command `--use-system-ssl`.

Checking the Web Host's Availability over the Secure HTTPS Protocol

To get access to a web host over the HTTPS, do the following:

1. In the Internet Explorer address bar, type: `https://server_name`.
2. After you log on to the server, the web server page will be displayed.

If the connection to the web server could not be established, refer to the Problems and Troubleshooting (on page 150).

Problems and Troubleshooting

Checking the Program Components Integrity	151
The Program Won't Start	152
ViPNet CSP Conflicts with Other Programs	154
Can't Use Accord-TSHM Electronic Lock	156
When You Are Using eToken Aladdin, the System Irresponsive	157
Unable to Check the Certificate	158
Document Can't be Encrypted	159
Can't Use the Digital Signature	163
No Connection to the Server over HTTPS	165
When You Connect to a Server, Security Warning Is Displayed	170
Providing Additional Information About the Problem	171

Checking the Program Components Integrity

For visual monitoring of the libraries availability:

1. In the main ViPNet CSP window, in the navigation pane, select **Details**.
2. In the **Executables** table, check the libraries list.

To check the libraries integrity:

1. In the main ViPNet CSP window, select **Details**.

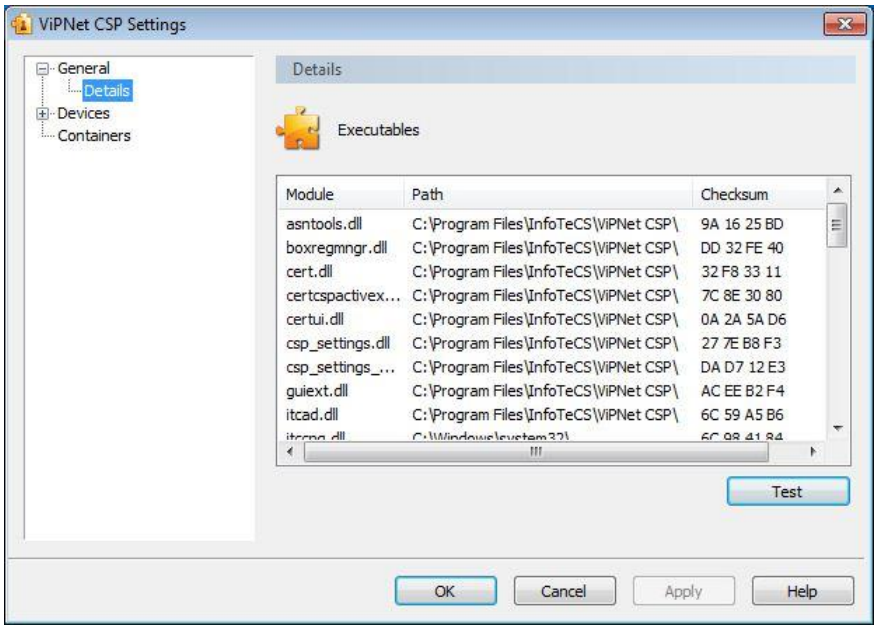

Figure 70: The Details pane

2. Click **Test**.

   Thus, you force recalculation of checksums and the check of their conformity to the sums specified in each of the modules.

   After the check is finished, results of the check will be displayed.

The Program Won't Start

If, on the ViPNet CSP program start, you are notified that the integrity check has failed or that some components are missing, then you can't work with the program.

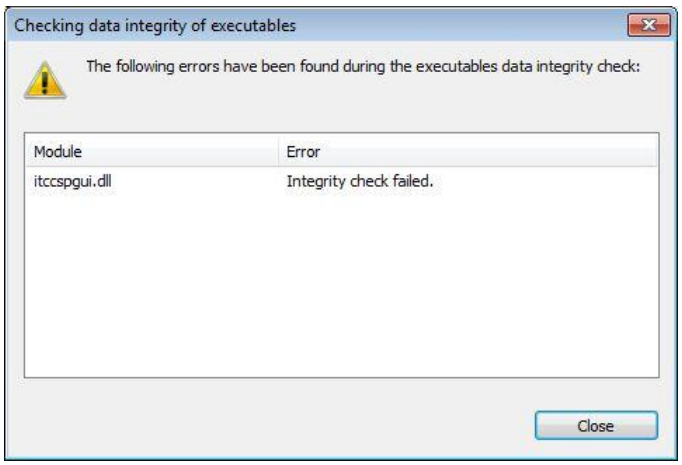

Figure 71: Error messages on the ViPNet CSP program start

To restore the operability of ViPNet CSP, install the program again over the previous version (without removing it). To do that:

1. Click the `Setup.exe` file .
2. In the **ViPNet CSP Installation** window, select **Upgrade**, and then click **Continue**. The program components' upgrading will start.

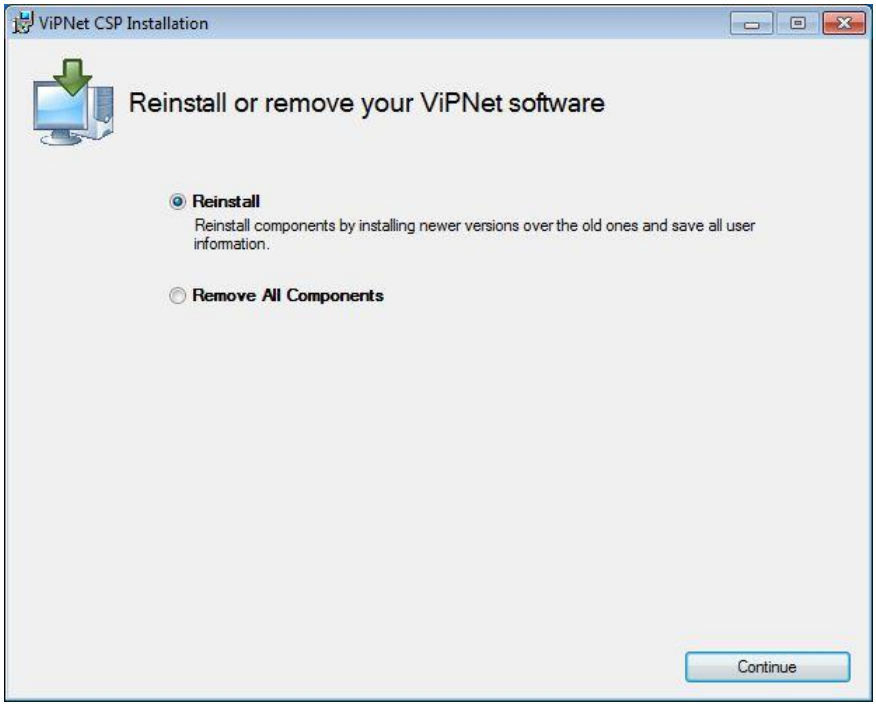
ViPNet CSP Installation
Reinstall or remove your ViPNet software
Reinstall
Reinstall components by installing newer versions over the old ones and save all user information.
Remove All Components
Continue

Figure 72: Updating ViPNet CSP

3 After upgrading is finished, you will be prompted to restart your computer. In the restart message, click **Yes**.

After restart the ViPNet CSP program will be fully operational. If the program has been registered earlier, you don't need to register it again.

ViPNet CSP Conflicts with Other Programs

ViPNet software peculiarities may lead to some failures in the operability of some third-party programs.

To eliminate any conflicts between ViPNet software and third-party programs, make some changes in the Windows system registry:

1. Click the **Start** button. In the search box, type run, and then, in the list of results, click **Run**.
2. In the **Open** box, type `regedit` and click **OK**. The registry editor window will be displayed.

Warning: Do not change any other system registry parameters but `Flags`. An incorrect change in the registry may lead to computer malfunction.

3. Under the registry key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\infotecs\PatchEngine`, set the `Flags` parameter value to 0.
4. Restart your computer.

   If you have applied the changes, but the problem still arises, contact Infotecs technical support.

If ViPNet CSP conflicts with third-party cryptographic service providers, you may disable ViPNet CSP work via the MS Crypto API interface.

Warning: After disabling the MS Crypto API interface support, you can't use ViPNet CSP cryptographic functions in Microsoft Office programs and other applications, which use this interface. However, you still may use ViPNet CSP functions in various ViPNet programs.

To disable the work of ViPNet CSP via the MS Crypto API interface, in the **General** (see figure on page 32) section, clear the **Allow ViPNet CSP to use MS Crypto API** check box. The change will take effect when you restart Windows.

Can't Use Accord-TSHM Electronic Lock

If “Accord-TSHM” electronic lock is installed on your computer, but you can't use it in ViPNet CSP as a random numbers generator, do the following:

1. Make sure that drivers for the “Accord-TSHM” electronic lock are installed on your computer.
2. Copy the `tmdv32.dll` file from the drivers installation folder (by default `C:\Accord`) to the following folder:
   - If you use a 64-bit Windows OS, copy the file to the `C:\Windows\System32` folder.
   - If you use a 32-bit Windows OS, copy the file to the `C:\Windows\SysWOW64` folder.
3. In ViPNet CSP, choose “Accord-TSHM” as a random number generator (see Using a Random Number Generator on page 89).

When You Are Using eToken Aladdin, the System Irresponsive

If you are using an eToken Aladdin device and your system irresponsive, make sure that eToken PKI Client 5.1 (or later) software have been installed.

Unable to Check the Certificate

During the certificate's installation, the certificate verification error may occur. This means that the issuer's certificate and CRL have not been installed in the system (see Installing Issuer's Certificates and CRL on page 73).

Document Can't be Encrypted

Email Address of the Certificate Is Not Found on the List of Contact Addresses

During the certificate's import to the contact the following message may be displayed:

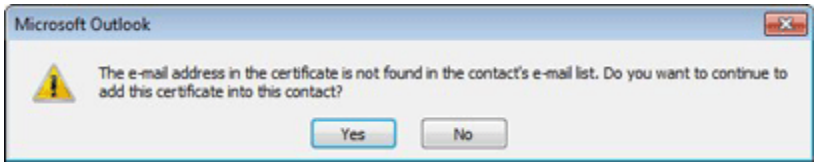
Microsoft Outlook
The e-mail address in the certificate is not found in the contact's e-mail list. Do you want to continue to add this certificate into this contact?
Yes
No

Figure 73: Certificate import error

This means that the certificate does not contain an email address, which corresponds to this contact's address. That's why you can't encrypt a message using this certificate.

Possible reasons and ways of solving the problem:

- If the certificate does not belong to this contact:
  - Open the **Certificate** window by double-clicking the certificate file on your hard drive.

- On the **General** tab, make sure that this certificate is intended for the contact in question. If not, select the certificate you want to import.

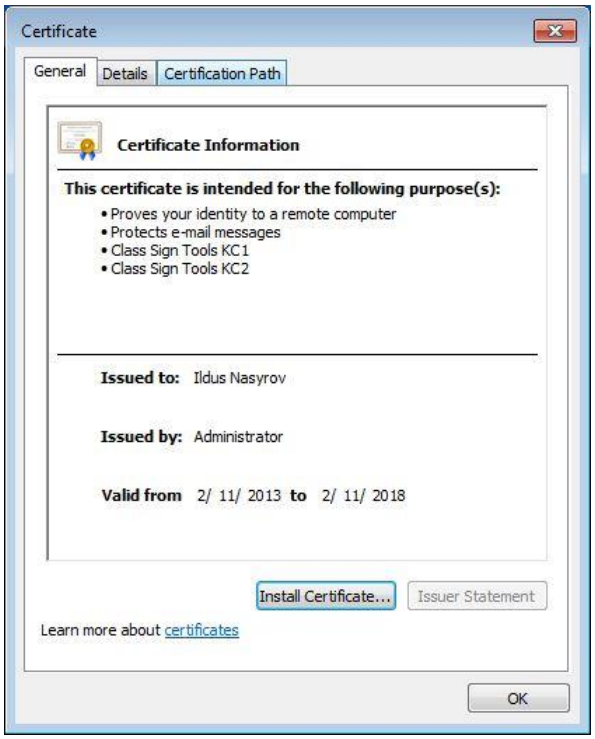

Figure 74: Certificate's owner verification

- If the certificate does not contain the email address of this contact:
  - Open the **Certificate** window by double-clicking the certificate file on your hard drive.

- On the **Details** tab, click the **Subject** box and make sure, that the **E** parameter has the correct email address as its value.

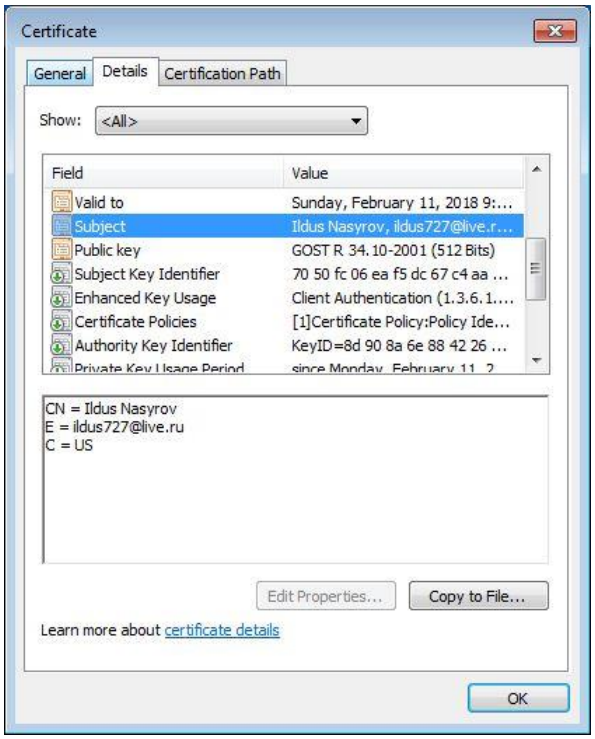

Figure 75: Certificate email address check

- If not, create a request for a new certificate:
  - the recipient, if you have imported the contact's certificate;
  - the administrator of your Certification authority, if you have added your certificate to the system store.

Invalid Certificate

During an encrypted message sending, the warning message may be displayed:

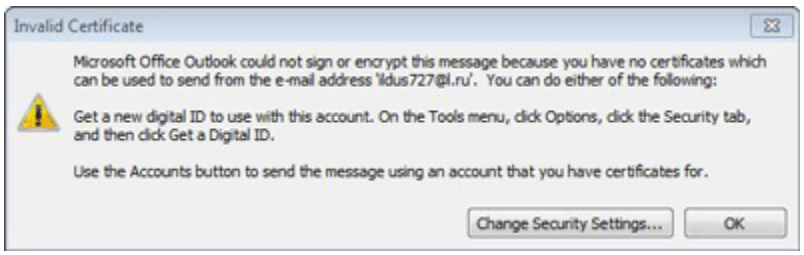
Invalid Certificate
Microsoft Office Outlook could not sign or encrypt this message because you have no certificates which can be used to send from the e-mail address 'ildus727@l.ru'. You can do either of the following:
Get a new digital ID to use with this account. On the Tools menu, click Options, click the Security tab, and then click Get a Digital ID.
Use the Accounts button to send the message using an account that you have certificates for.
Change Security Settings...
OK

Figure 76: The message about invalid certificate in Outlook 2003

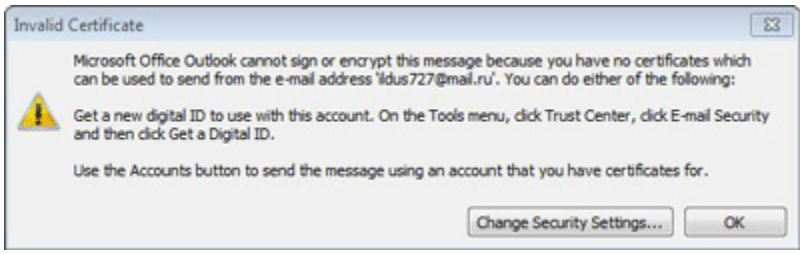
Invalid Certificate
Microsoft Office Outlook cannot sign or encrypt this message because you have no certificates which can be used to send from the e-mail address 'ildus727@mail.ru'. You can do either of the following:
Get a new digital ID to use with this account. On the Tools menu, click Trust Center, click E-mail Security and then click Get a Digital ID.
Use the Accounts button to send the message using an account that you have certificates for.
Change Security Settings...
OK

Figure 77: The message about invalid certificate in Outlook 2007

The reason may be as follows:

- The recipient's certificate does not contain the email address of this recipient (see Email Address of the Certificate Is Not Found on the List of Contact Addresses on page 159).
- Your certificate does not contain your email address (see Email Address of the Certificate Is Not Found on the List of Contact Addresses on page 159).
- The recipient's certificate or your certificate is invalid. Request a new certificate from the recipient or from the administrator of your Certification authority.
- The certificate for signing and encrypting (see Advanced Configuring of Digital Signature and Encryption on page 109) is not specified.
- The issuer's certificate is not installed (see Installing Issuer's Certificates and CRL on page 73) in the system store.

Can't Use the Digital Signature

The Corresponding Private Key Is Not Found

When you are choosing a certificate for signing, the **ViPNet CSP - Key Container Initialization** window may be displayed, which means that the private key corresponding to the chosen certificate is not found. This may happen if the private key container has been disabled in the ViPNet CSP program (see Deleting a Container on page 82).

To sign a document using the chosen certificate, in the **ViPNet CSP - Key Container Initialization** window, specify the path to the private key container and its certificate. If you don't know the container's location, you can't use the chosen certificate.

If, in the **ViPNet CSP - Key Container Initialization** window, you specify the keys container location, this container will be added to the list on the **Containers** tab.

The Email Message Can't be Signed

When you are signing an email message, you may be notified that there is no any certificate containing your email address. In this case, you should ask the Key and Certification Authority for such a certificate. Your email address and “Secure Email” attribute in Enhanced Key Usage field should be specified in the certificate.

An Email Message Is Signed with a Certificate That You Have Not Selected for Signing

Such an error occurs when the certificate chosen for signing does not contain its owner's email address or the specified address does not correspond to the outgoing message's address. Moreover, when the message is signed, a different certificate that contains the sender's email address is chosen from the system store.

To resolve this error:

1. Create a new certificate request and specify the correct email address in it.
2. Send the certificate request to the administrator of your Certification authority and wait until receive a new certificate.
3. Specify the received certificate as a certificate for signing.

Macros or Microsoft Access 2007 Database Can't be Signed

When you are signing a macros or a Microsoft Access 2007 package, there may be no certificates that you can select for signing. Thus, you can't sign a code. To eliminate the problem, ask your Key and Certification Authority for a certificate with a Code signing attribute in the Enhanced Key Usage field.

The Signature Line in Microsoft Word 2003 or Excel 2003 Can't be Signed

You can't sign a signature line in Microsoft Word and Excel versions earlier than Microsoft Office 2007. To sign a signature line, you need to open a document in Microsoft Office 2007.

Signed Microsoft Word or Excel Document Can't be Edited

To edit a signed Microsoft Word or Excel document, you need to remove a digital signature (see Removing a Digital Signature on page 99) and then make necessary changes. After that you can sign this document again.

Warning: We strongly recommend you not to remove a digital signature from a document, which was signed by another person, if this document has legal validity.

No Connection to the Server over HTTPS

The IIS Server and the Web Client Have Different ViPNet CSP Versions

On the web client, you need to install the same version of the software as on the server.

User's Certificates, the Issuer's Certificate, and CRL Were Installed in the Wrong Store

Check that the certificates are installed in the required store using the standard MMC (Microsoft Management Console).

To view certificates installed in a system store:

1. Open the MMC:
   - Press **Win**+**R**.

     On the **Start** menu, select **Run**.
   - In the **Open** box, type `mmc`, and click **OK**.
2. On the **File** menu, select **Add/Remove Snap-in**.
3. In the **Add/Remove Snap-in** window, in the **Available snap-ins** list, select **Certificates**, and click **Add**.
4. In the **Certificates snap-in** window, choose snap-in type, that you want to add:
   - **My user account**, to view web client's certificates;
   - **Computer account**, to view server's certificates;

Note: If you don't want to add a **Certificates** snap-in to the console every time you need it, you may save it. To do this, on the **File** menu, click **Save**.

User's certificates, issuer's certificate and CRL should be installed in the correct system store, and when you open them there should be no errors.

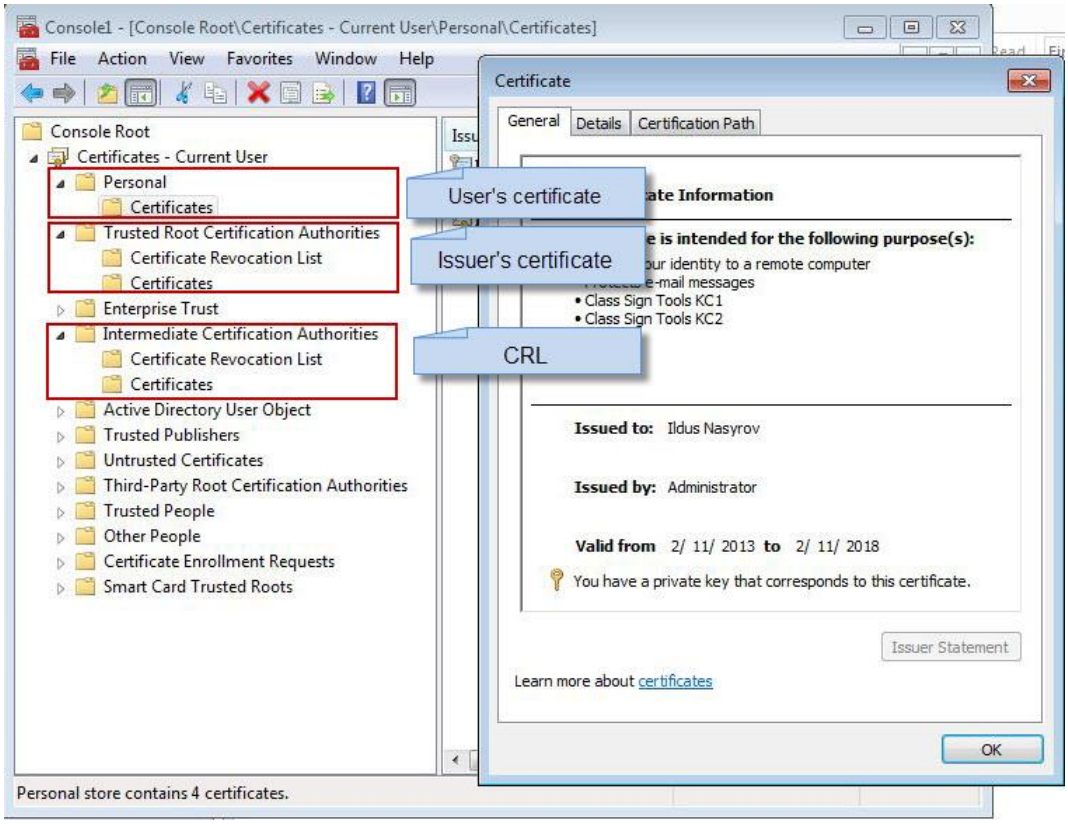

Figure 78: Web client certificate is in the current user's system store

In the MMC snap-in, the following local computer certificates should be added for the IIS:

- The **Personal > Certificates** section should contain a user's (server's) certificate.
- The **Trusted Root Certification > Certificates** section should contain the issuer's certificates.
- The **Intermediate Certification Authorities > Certificate Revocation List** section should contain the CRL.

In the MMC snap-in, the following current user's certificates should be added for the web client:

- The **Personal > Certificates** section should contain a user's (web-client) certificate.
- The **Trusted Root Certification > Certificates** section should contain the issuer's certificates.

- The **Intermediate Certification Authorities > Certificate Revocation List** section should contain the CRL.

If a certificate is not installed or has been installed incorrectly, you need to install or reinstall it correctly in the system store (see Installing Issuer's Certificates and CRL on page 73).

The Browser Is Not Configured to Work over the TLS Protocol

By default Internet Explorer settings allow you to work over encrypted TLS protocol. If you can't connect to the server, make sure that the necessary certificate is added to the web browser and the TLS/SSL protocol is enabled in the browser settings.

To check that the certificate is added to your web browser:

1. In the Internet Explorer browser, on the **Tools** menu, click **Internet Options**.
2. In the **Internet Options** window, on the **Content** tab, click **Certificates**.
3. In the **Certificates** window, on the **Personal** tab, make sure that necessary certificate is present on the list.
4. Choose the certificate and click **View**.
5. In the **Certificate** window, make sure that the certificate contains the **Client Authentication attribute** (see figure on page 168). If your certificate does not contain this attribute, ask for a certificate with this attribute in the Key and Certification Authority (see “ViPNet Administrator Key and Certification Authority. Administrator’s Guide”).

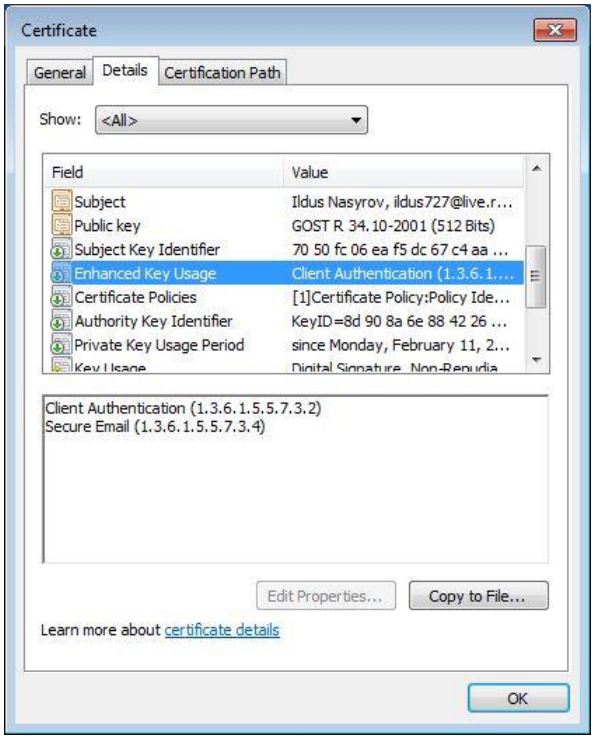

Figure 79: Web client certificate details

To check the TLS/SSL protocol activity:

1. In the Internet Explorer browser, on the **Tools** menu, click **Internet Options**.
2. In the **Internet Options** window, click the **Advanced** tab.
3. Make sure that the **SSL 3.0**, **TLS 1.0** check boxes are selected, and the **SSL 2.0** check box is cleared.
4. Check connection to the web server.

The IIS Services Should Be Restarted

In some cases, you need to restart the IIS service to connect to a server over the newly configured TLS protocol. To do this:

1. Open the **Windows Task Manager** window.
2. End the `inetinfo.exe` process.
3. After the service has started automatically, check the connection to a server.

Password to Server's Certificate Should Be Saved

In some cases, to access the server you need to save the key container password. To do this:

1. In the MMC snap-in, open a certificate.
2. In the **Certificate** window, on the **Details** tab, click **Copy to File**.
3. On the start page of the **Certificates Export Wizard**, click **Next**.
4. In the key container logon window, type the server's user password and select the **Save Password** and the **Do not show this window again** check boxes.
5. Click **OK**. Now you can close the wizard, the password has been saved.

When You Connect to a Server, Security Warning Is Displayed

When you are connecting to the server, a **Security warning** may be displayed by your web browser: “Specified in the certificate name is incorrect or does not match the name of the site”. In this case, check that the server domain name is the same as the name of the user this certificate is issued for.

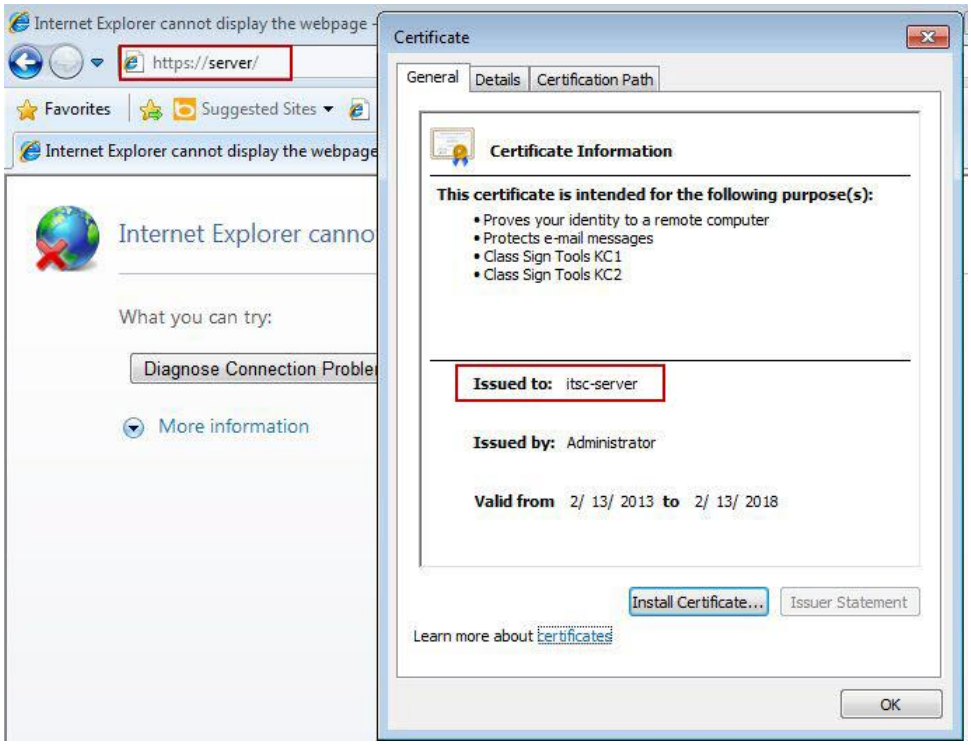

Figure 80: Security warning about names mismatch

Providing Additional Information About the Problem

A specialist of the Infotecs technical support may ask you to provide more information to solve the problem. In this case:

1. Press **Win**+**R**.

   On the **Start** menu, select **Run**.

2. In the **Open** box, type `regedit` and press **Enter**.

3. In the **Registry Editor** program, go to the `Logs` folder, which is accessible by the following path:

   - in the 32-bit Windows OS: `HKEY_LOCAL_MACHINE\SOFTWARE\infotecs\Logs`;
   - in the 64-bit Windows OS: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\infotecs\Logs`.

4. Change the `Level` and `dbg_level` values to `0xff (255)`.

5. Restart your computer.

Note: It may take a long time to start your computer.

6. Download the DebugView http://technet.microsoft.com/ru-ru/sysinternals/bb896647.aspx program.

7. Run `DbgView.exe` as a system administrator.

8. Repeat the steps that have caused the problem.

9. In the DebugView program, select all strings and copy them to a text file.

10. Add this text file to an archive and send it to the support with a description of the problem.

Note: If third-party software is required to reproduce the problem, you should note it in your email.

11 Set the `dbg_level` key value to 0.

12 Restart your computer.

External Storage Devices

Overview

External storage devices are designed for storing key containers (see Key container on page 178) that you can use for authentication, digital signing (see Digital signature on page 178), or other purposes.

On an external device, you can store keys created using different encryption algorithms in ViPNet software or third-party programs. Maximum number of key containers stored on a device depends on the device's memory space.

ViPNet software supports two authentication methods involving external storage devices:

- ViPNet user's personal key stored on an external device with the following limitations:
  - Each external storage device can be used for authentication of only one ViPNet user.
  - Each external storage device can be used for authentication of one ViPNet user on several ViPNet hosts.
  - If you use this authentication method, then store your digital signature keys (created in a certification authority using ViPNet software) and the personal key on one external storage device.
- Certificate with its private key stored on an external device.

  You can request for the certificate in Windows domain and store the corresponding key container on your external storage device that supports PKCS#11.

You can perform all the required configuring concerning key containers and external storage devices in the ViPNet CSP program. Make sure that you've installed the drives required for your external device. Before you store keys on your device, make sure that the device is formatted.

Supported External Storage Devices

In the table below, you can find the list of devices supported by the ViPNet software. For each external device, the table contains description, conditions, operation specifics, and information on PKCS#11 standard support.

Note: PKCS#11 (also known as Cryptoki) is one of the PKCS standards (Public Key Cryptography Standards — cryptographic standards of public keys) developed by the RSA Laboratories company. The standard defines the API interface independent of the platform and intended for the work with cryptographic devices of identification and data storage.

Table 5: Supported external devices

Device name in ViPNet CSP	Device name and type	Requirements	PKCS#11 support
eToken Aladdin	**eToken PRO (Java)**, **eToken PRO** personal electronic keys, **eToken PRO (Java)**, **eToken PRO** smart cards by Aladdin Company	The PKI Client software of the 5.1 version or later should be installed on the computer. **Note:** You can use eToken PRO SmartCard with any standard PC/SC-compatible USB card reader.	Yes
iButton Aladdin	**iButton (Dallas)** electronic keys of the **DS1993**, **DS1994**, **DS1995**, and **DS1996** types	A reader device must be connected to the computer. The 1-Wire Drivers software version 3.20 or 4.0.3, which ensures data exchange with iButton, should be installed on the computer.	No
Smartcard Athena	Smartcards with memory of the I2C (ASE M4) type, synchro cards with a 2/3 bus and protected memory meeting the requirements of the ISO7816-3 (ASE MP42) standard	The ASEDrive III PRO-S reader by Athena company is used to process data on a smart card. Drivers of the 2.6 version should be installed on the computer.	No

Siemens CardOS	**CardOS/M4.01a**, **CardOS V4.3B**, **CardOS V4.2B**, **CardOS V4.2B DI**, **CardOS V4.2C**, and **CardOS V4.4** smart cards by Atos (Siemens)	Siemens CardOS API V5.0 and later should be installed on the computer.	Yes

Note: For each device, the list of supported operating systems is available on the manufacturer's official web page.

Glossary

C

CA administrator

An authorized person privileged to sign certificates on behalf of a certification authority.

See also: Certification authority (CA) (on page 177).

Certificate request

A message protected with a digital signature that contains the user name, the public key and its properties, the desired validity period of the certificate, certificate intended purposes, and some other information (depends on the request format and the software used to create the request).

See also: Digital signature (on page 178), Private key (on page 179), Public key (on page 179), Public key certificate (on page 179).

Certificate revocation list (CRL)

A list of certificates that have been revoked or held by the Certification Authority administrator, and are not valid at the moment specified in this certificate revocation list.

See also: CA Administrator (on page 177), Certificate hold, Certificate revocation.

Certification authority (CA)

An entity that issues digital certificates, including public key certificates. In ViPNet networks, certificates are issued in Key and Certification Authority.

See also: Public key certificate (on page 179), ViPNet Key and Certification Authority, ViPNet network.

D

Digital roulette

An integrated ViPNet software component which allows you to launch a random number generator based on your chance movements.

Digital signature

An attribute of an electronic document intended to protect the document authenticity. It is generated when encrypting information using a private key of a digital signature. A digital signature identifies the public key certificate owner, as well as proves non-repudiation of the document contents.

See also: Private key (on page 179), Public key certificate (on page 179).

I

Issuer's certificate

A certificate of a Certification Authority administrator that is used for verifying other certificates issued by this CA.

See also: Public key certificate (on page 179).

K

Key container

A file where a private key and the corresponding public key certificate are stored.

See also: Public key certificate (on page 179).

P

PKI (public key infrastructure)

A set of hardware, software, policies, and procedures intended for creating, managing, distributing, using, storing, and revoking public key certificates, binding public keys with respective user identities by means of a certification authority.

See also: Certification authority (CA) (on page 177), Public key (on page 179), Public key certificate (on page 179).

Private key

The secret part of a key pair used in asymmetric encryption. A private key is intended to generate a digital signature that can be verified by the corresponding public key and to decrypt a received message encrypted by using the corresponding public key.

A digital signature key is a private key.

See also: Digital signature (on page 178), Public key (on page 179).

Public key

An asymmetric encryption key, one of an asymmetric keys pair. It needs not to be kept secret and can be distributed freely and published in a network accessible directory. A public key is used to verify digital signature. In ViPNet CSP, it is used for encryption.

See also: Digital signature (on page 178).

Public key certificate

An electronic document of a previously specified format that uses a digital signature to bind a public key with an identity, information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual. A certificate contains information about the key owner, the public key, about its purpose and usage, about the certification authority that has issued the certificate, the certificate validity period, and some other parameters. In a ViPNet network, certificates are issued in ViPNet Key and Certification Authority or in ViPNet Network Manager and verified with the digital signature of the ViPNet Key and Certification Authority administrator or ViPNet Network Manager administrator. This provides authenticity and integrity of the information specified in the certificate, including its public key and description of its subject.

See also: Digital signature (on page 178), Public key (on page 179), ViPNet Key and Certification Authority, ViPNet Key and Certification Authority administrator.

R

Root certificate

A self-signed certificate of a ViPNet network administrator that is the top one in the certificate trust chain. In other words, there is no certificate you can validate a root certificate with. Root certificates are used to validate ViPNet user or issuer's certificates.

See also: Public key certificate (on page 179).

Index

A
Adding a Digital Signature to a Message • 108, 109
Adding a Digital Signature to All Messages • 108, 118
Advanced Configuring of Digital Signature and Encryption • 108, 120, 123, 125, 126, 164

B
Buying Program (Getting a Serial Number) • 36, 39, 41, 51

C
CA administrator • 179
Certificate revocation list (CRL) • 18, 23
Certification authority (CA) • 179, 181
Checking the Web Host's Availability over the Secure HTTPS Protocol • 148, 149, 150
Configuring a Client Host • 147
Configuring a Server Host • 147
Creating a Backup Copy of a Container • 83
Creating a Certificate Request and Generating a Private Key • 18, 53, 148, 149

D
Deleting a Container • 165
Digital roulette • 57
Digital signature • 11, 175, 179, 181
Digital Signature and Encryption in Microsoft Mail Programs • 22
Digital Signature in Microsoft Office Documents • 22
Digital Signature in Microsoft Office InfoPath • 22
Digitally Sign/Sign Button Isn't Displayed • 118

E
Email Address of the Certificate Is Not Found on the List of Contact Addresses • 109, 110, 164
Email Encryption • 22, 108, 113, 129
Encrypting Documents and Files • 108
Exchanging Certificates with the Message Recipient • 108

I
If the Configuration of Your Computer Has Been Changed • 35
Installing a Certificate from Container • 24, 63, 64, 66, 69
Installing a Certificate Which Has Not Been Added to the Container • 69
Installing Certificates in a Container • 53, 61, 148, 149
Installing Container from a Folder • 18, 59, 61, 71
Installing Container from an External Device • 18, 61, 71
Installing Containers and Certificates • 18, 32

Installing Issuer's Certificates and CRL • 18, 24, 53, 61, 64, 66, 72, 73, 108, 148, 149, 160, 164, 169
Installing the User Certificate in the System Store • 18, 53, 57, 61, 62, 73, 148, 149
Issuer's certificate • 18, 23

K
Key container • 175
Key Container • 20, 69

M
Macro Digital Signature • 22, 144

O
Obtaining and Installing a Private Key and a Certificate • 18, 23
Organizing a Protected Connection via TLS/SSL • 22, 24

P
Private key • 179, 180
Problems and Troubleshooting • 123, 151
Public key • 179, 181
Public key certificate • 16, 179, 180, 181, 182

R
Receiving Your Registration Code from the Administrator • 38, 51
Registering ViPNet CSP • 33, 36, 43, 44, 46
Removing a Digital Signature • 95, 96, 106, 166
Requesting a Registration Code • 36, 37, 49
Requesting Your Registration Code by Email • 38
Requesting Your Registration Code by Phone • 38
Requesting Your Registration Code on the Internet (online) • 38, 41, 45

S
Saving Registration Data • 35, 41, 44, 48
Setting Up and Starting ViPNet CSP • 148, 149
Starting the Registration Process • 37, 47
Supported External Storage Devices • 12, 65, 71
System Administrator Actions for Registration Using a File • 35, 44

U
Using a Random Number Generator • 158

V
Viewing a Digital Signature • 106
Viewing and Configuring Container Properties • 85
Viewing the Encrypted Messages • 108
ViPNet CSP Licensing • 31, 35
ViPNet CSP Purpose • 11, 23
ViPNet CSP Scope • 24, 64, 66, 72, 75
ViPNet CSP Setup • 23

W
Ways to Install a Private Key and a Certificate • 24, 108